НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК 004.056

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження та шляхи розв'язання проблем сертифікації інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Регламенту ЄС 2019/881»

Виконав:
студент II курсу, групи ТС-91мп
Бруско Віталій Миколайович _____

Керівник:
д.т.н., професор Горицький В.М _____

Рецензент:
д.т.н., професор Коновалов О.Ю _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Бруско Віталію Миколайовичу

1. Тема дисертації «Дослідження та шляхи розв'язання проблем сертифікації інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Регламенту ЄС 2019/881», науковий керівник дисертації Горицький Віктор Михайлович, д.т.н., професор, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження - національна система кібербезпеки України.

4. Предмет дослідження - сертифікація інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

5. Перелік завдань, які потрібно розробити:

а) дослідження шляхів забезпечення кібербезпеки та підвищення рівня довіри до цифрових технологій в ЄС;

б) аналіз завдань ENISA в галузі кібербезпеки згідно Акту про кібербезпеку (Регламент ЄС 2019/881);

в) дослідження ролі Європейської системи сертифікації кібербезпеки у підвищенні довіри та безпеки до інформаційних та телекомунікаційних технологій у відповідності до Акту про кібербезпеку (Регламент ЄС 2019/881);

г) вдосконалення національної системи кібербезпеки України шляхом дослідження та розв‘язання проблем сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС;

д) розробка вимог до структури та ресурсів органу з сертифікації кібербезпеки національної системи кібербезпеки України;

е) розробка процедури сертифікації інформаційних та телекомунікаційних технологій в національній системі кібербезпеки України.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

7. Орієнтовний перелік публікацій

8. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Затвердження теми з науковим керівником	01.04.2020	
2	Перший розділ	08.06.2020	
3	Другий розділ	16.09.2020	
4	Третій розділ	01.11.2020	
5	Кінцевий термін подачі на кафедру ДР	10.12.2020	
6	Державна атестація (комплексний державний екзамен та захист дипломної роботи)	22.12.2020	

Студент В. М. Бруско

Науковий керівник дисертації В. М. Горицький

РЕФЕРАТ

Темою магістерської дисертації є дослідження та шляхи розвязання проблем сертифікації інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Регламенту ЄС 2019/881.

Робота містить 128 сторінок, зокрема 11 ілюстрацій та 13 джерел інформації.

Тема магістерської дисертації є актуальною, так як гостро стоїть питання щодо вдосконалення національної системи кібербезпеки України шляхом дослідження та розв‘язання проблем сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

Мета дисертації полягає у вдосконаленні національної системи кібербезпеки України.

Об’єктом дослідження є національна система кібербезпеки України.

Предмет дослідження - сертифікація інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

У дисертації була запропонована методика вдосконалення національної системи кібербезпеки України шляхом дослідження та розв’язання проблем сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС. Були надані рекомендації щодо створення гармонізованої з європейською національної системи сертифікації кібербезпеки.

ABSTRACT

The topic of the master's dissertation is research and ways to solve problems of certification of information and telecommunications technologies in Ukraine on cybersecurity in accordance with the requirements of EU Regulation 2019/881.

The work contains 128 pages, including 11 illustrations and 13 sources.

Theme of master's thesis is relevant, as the issue of improving the national cybersecurity system of Ukraine by researching and solving problems of certification of information and telecommunications technologies on cybersecurity in accordance with the requirements of the EU Cybersecurity Act is acute.

The purpose of the dissertation is to improve the national cybersecurity system of Ukraine.

The object of research is the national cyber security system of Ukraine.

The subject of the research is the certification of information and telecommunication technologies in Ukraine on cybersecurity for compliance with the requirements of the EU Cybersecurity Act.

The dissertation proposed a method of improving the national cybersecurity system of Ukraine by researching and solving problems of certification of information and telecommunications technologies on cybersecurity in accordance with the requirements of the EU Cybersecurity Act. Recommendations were provided for the creation of a harmonized with the European national cybersecurity certification system.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ІКТ – Інформаційно-комунікаційні технології

IoT – Internet of Things - Інтернет речей

МСП – Малі та середні підприємства

ENISA – The European Union Agency for Cybersecurity - Агентство Європейського Союзу з питань мережевої та інформаційної безпеки

ECCG – Європейська група з сертифікації кібербезпеки

CSIRT – Computer security incident response team – Комп'ютерна група реагування на надзвичайні ситуації

НААУ – Національне агентство з акредитації України

GDPR – General Data Protection Regulation - Загальний регламент по захисту даних

ООВ – Органи з оцінки відповідності

CERT – Computer Emergency Response Teams - Комп'ютерна група реагування на надзвичайні ситуації

NLO – National Liaison Officers network – Національна Мережа Офіцерів зв'язку

ВСТУП

Питання кібербезпеки сьогодні є пріоритетним для ІТ-галузі як в теоретичному аспекті, так і в плані довіри до практично реалізованих систем кібербезпеки. Для України це ще й питання гармонізації національного законодавства з законодавством ЄС у відповідності до Угоди Україна – ЄС.

27 червня 2019 року в Європейському Союзі вступив в силу новий Регламент 2019/881 про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) і сертифікації з кібербезпеки інформаційних і комунікаційних технологій (ІКТ), більш відомий під назвою «Акт про кібербезпеку» (Cybersecurity Act) [3].

Як і GDPR (загальний регламент по захисту даних), Акт про кібербезпеку є частиною Європейської Стратегії Єдиного Цифрового Ринку. За оцінками Європейської Комісії, Єдиний Цифровий Ринок ЄС має потенціал стати найбільшим ринком онлайн бізнесу в світі та приносити приблизно 415 мільярдів Євро в економіку Європейського Союзу щорічно. За деякими підрахунками, оборот Єдиного Цифрового Ринку ЄС може досягти 1 трлн Євро вже у 2020 році. Для безлічі компаній такий цифровий ринок також відкриває великі можливості для пропозиції своїх послуг. Очікувано, що буде рости і попит на фахівців в сфері кібербезпеки та захисту даних.

Акт про кібербезпеку серед іншого встановлює і єдиний фреймворк сертифікації в сфері кібербезпеки для ІКТ. Цей фреймворк в першу чергу цікавий власникам і розробникам програмних рішень, які надають свої продукти або послуги в Європейському Союзі.

Метою Акту про кібербезпеку є розвиток і підтримка кібербезпеки ІКТ продуктів і послуг на ринку ЄС. Ключову роль в цьому процесі повинна виконувати ENISA, чиї повноваження були істотно розширені в зв'язку з прийняттям Акту.

Акт передбачає добровільну сертифікацію з кібербезпеки продуктів ІКТ, послуг ІКТ і процесів ІКТ. Проте, інші акти Європейського Союзу або держав-

членів можуть визначати сфери, в яких сертифікація продуктів, послуг або процесів буде обов'язковою. Згодом Європейська Комісія повинна оцінити ефективність такого підходу і встановити обов'язковість сертифікації в певних сферах діяльності, але вже зараз зрозуміло, що незабаром сертифікація з кібербезпеки стане стандартом роботи в країнах Європейського Союзу.

Згідно Акту про кібербезпеку сертифікація проводиться акредитованими органами відповідно до обраної схеми. ENISA розробляє такі схеми на підставі програми Європейської Сертифікації, яка повинна була бути підготовлена Європейською Комісією до 28 липня 2020 року і включатиме список продуктів, послуг і процесів, які можуть бути сертифіковані.

ENISA повинна підтримувати спеціальний сайт, присвячений сертифікації, на якому буде надана вся необхідна інформація.

Сертифіковані продукти, послуги та процеси повинні відповідати вимогам встановлених технічних регламентів і стандартів у сфері кібербезпеки.

Сертифікація визнається у всіх країнах ЄС, а максимальний термін її дії становить 5 років і може бути продовжений на тих же умовах.

Згідно Акту про кібербезпеку сертифікація застосовується до [3]:

а) продуктів ІКТ (наприклад, комп'ютери, цифрові телевізори, IoT і т.д.);

б) послуг ІКТ (наприклад, розробка ПО, консультаційні послуги в сфері IT, хостинг і т.д.);

в) процесів ІКТ (заходи, виконані для проектування, розробки, поставки або підтримки IT продуктів і послуг).

Питання сертифікації з кібербезпеки на сьогодні є вкрай важливим і разом з тим відкритим.

Сертифікація з кібербезпеки може бути цікава для власників і розробників програмних рішень, які надають свої продукти або послуги в Європейському Союзі. Особливо, це стосується продуктів і послуг в тих сферах, де кібербезпека або загроза кібератаки можуть нести серйозні ризики, наприклад: медицина, фінанси, банківська діяльність, інтернет речей тощо.

Сертифікація підтверджує технічну надійність продуктів, послуг, а також

процесів їх розробки і підтримки одночасно у всіх країнах ЄС.

Також варто враховувати, що сертифікація може служити додатковим доказом того, що розробник IT рішень виконує вимоги GDPR, так як один з обов'язків, передбачених GDPR, - прийняття необхідних технічних заходів для забезпечення безпеки роботи з персональними даними.

Акт з кібербезпеки встановлює три можливих рівні сертифікації: базовий, суттєвий, високий.

Рівень сертифікації залежить від рівня ризику, пов'язаного з передбачуваним використанням продукту ІКТ, послуг ІКТ або процесу ІКТ. Рівень також залежить від таких факторів, як:

а) вид даних, які обробляються;

б) обсяг даних;

в) ймовірність виникнення інциденту/атаки;

г) можливі наслідки інциденту/атаки.

Програма Європейської Сертифікації, розроблена Європейською Комісією, може передбачати самостійну сертифікацію виробників і постачальників продуктів, послуг або процесів. Така самостійна сертифікація можлива тільки для базового рівня сертифікації, як описувалося вище.

Для цього виробник або постачальник повинен надати в національний орган по сертифікації кібербезпеки наступне:

а) заяву про відповідність;

б) технічну документацію;

в) іншу необхідну інформацію.

Копія заяви про відповідність також направляється в ENISA.

Ухвалення Акта про кібербезпеку, а також єдиних в рамках ЄС схем сертифікацій з кібербезпеки дозволить значно поліпшити протидію кібератакам і захист даних. Також, єдині стандарти з кібербезпеки в усіх країнах ЄС значним чином сприятимуть розвитку Єдиного Цифрового Ринку в ЄС і довірі користувачів до цифрових послуг.

Це дозволить компаніям, які працюють на ринку ЄС та України, вирішити

проблему сертифікації своїх продуктів ІКТ, послуг ІКТ або процесів ІКТ відповідно до Акту ЄС про кібербезпеку, а інженерам – розвивати експертизу в сфері кібербезпеки та захисту даних з урахуванням нововведень.

Акт ЄС про кібербезпеку несе також переваги для громадян і бізнесу. Нові правила допоможуть людям довіряти пристроям, які вони використовують кожен день, тому що вони можуть обирати між продуктами, такими як пристрої Інтернету речей, які підпадають під загрози кібербезпеки.

Система сертифікації стане універсальним центром сертифікації кібербезпеки, що призведе до значної економії коштів для підприємств, яким в іншому випадку довелося б подавати заявки на отримання кількох сертифікатів в декількох країнах. Єдина сертифікація також усуне потенційні бар'єри для входу на ринок. Більш того, компанії будуть зацікавлені в інвестуванні в кібербезпеку своїх продуктів і перетворюють це в конкурентну перевагу.

Разом з тим, на сьогодні є потужні проблеми сертифікації в сфері кібербезпеки для ІКТ в Україні.

Суть її полягає в наступному. В сучасному суспільстві довіра та конкурентні переваги, в тому числі і для сертифікації кібербезпеки, досягаються шляхом її гармонізації з вимогами глобальної системи Інфраструктури якості, яка реалізується шляхом укладання багаторівневої низки відповідних Угод, як показано на рис 2.2 цієї магістерської роботи.

В Україні на сьогодні відсутні органи з сертифікації/органи з оцінки відповідності (ООВ) в сфері кібербезпеки для ІКТ, діяльність яких охоплюється цією Глобальною системою.

Разом з тим, Україна на сьогодні має всі Угоди, показані на рис. 2.3 цієї магістерської роботи, необхідні для застосування сертифікації з кібербезпеки ІКТ.

Таким чином, на внутрішньонаціональному рівні на сьогодні стає можливим застосування сертифікації з кібербезпеки ІКТ у спосіб, який дозволить такі сертифікації зробити визнаними в Глобальній Інфраструктурі якості.

Але, методологічно це потребує вирішення низки задач:

а) розробки схем сертифікації в сфері кібербезпеки ІКТ;

б) методичного забезпечення в сфері акредитації ООВ кібербезпеки ІКТ для Національного агентства з акредитації України (НААУ);

в) забезпечення визнання результатів акредитації ООВ кібербезпеки ІКТ та сертифікації кібербезпеки ІКТ на глобальному (Європейському) рівнях.

Тому, в магістерській роботі вирішується актуальна наукова задача – вдосконалення національної системи кібербезпеки України шляхом дослідження та розв‘язання проблем сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

Мета роботи – вдосконалення національної системи кібербезпеки України.

Об‘єкт дослідження – національна система кібербезпеки України.

Предмет дослідження – сертифікація інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

Наукові задачі дослідження:

ж) дослідження шляхів забезпечення кібербезпеки та підвищення рівня довіри до цифрових технологій в ЄС;

з) аналіз завдань ENISA в галузі кібербезпеки згідно Акту про кібербезпеку (Регламент ЄС 2019/881);

и) дослідження ролі Європейської системи сертифікації кібербезпеки у підвищенні довіри та безпеки до інформаційних та телекомунікаційних технологій у відповідності до Акту про кібербезпеку (Регламент ЄС 2019/881);

к) вдосконалення національної системи кібербезпеки України шляхом дослідження та розв‘язання проблем сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС;

л) розробка вимог до структури та ресурсів органу з сертифікації кібербезпеки національної системи кібербезпеки України;

м) розробка процедури сертифікації інформаційних та телекомунікаційних технологій в національній системі кібербезпеки України.

1 ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПІДВИЩЕННЯ РІВНЯ ДОВІРИ ДО ЦИФРОВИХ ТЕХНОЛОГІЙ В ЄС

1.1 Мережеві й інформаційні системи та електронні комунікаційні мережі й послуги як основа економічного зростання та кіберзагроз для ЄС

Мережеві й інформаційні системи та електронні комунікаційні мережі й послуги відіграють життєво важливу роль у житті суспільства і стали основою економічного зростання. Інформаційно-комунікаційні технології (ІКТ) лежать в основі складних систем, що підтримують повсякденну суспільну діяльність, підтримують роботу наших економік у таких ключових секторах, як охорона здоров'я, енергетика, фінанси та транспорт, і, зокрема, підтримують функціонування внутрішнього ринку.

Зараз використання мереж та інформаційних систем громадянами, організаціями та бізнесом у всьому Європейському Союзі є поширеним. Оцифровка та підключення стають основними характеристиками постійно зростаючої кількості продуктів та послуг, і з появою Інтернету речей (IoT), як очікується, протягом наступного десятиліття по всьому ЄС буде розгорнуто надзвичайно багато підключених цифрових пристроїв. Незважаючи на те, що все більше пристроїв підключено до Інтернету, безпека та стійкість недостатньо вбудовані в проект, що призводить до недостатньої кібербезпеки. У цьому контексті обмежене використання сертифікації призводить до того, що окремі, організаційні та бізнес-користувачі мають недостатньо інформації про особливості кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, що підриває довіру до цифрових рішень. Мережеві та інформаційні системи здатні підтримувати всі аспекти життя та стимулювати економічне зростання ЄС. Вони є основою для досягнення єдиного цифрового ринку.

Разом з тим, в області IoT, мабуть, найменше порядку в плані забезпечення інформаційної безпеки. Сьогодні ми спостерігаємо технологію, що потужно розвивається, але постійно мінливий ландшафт цієї галузі, прогнози тощо, часом

відводять убік від реальності, десятки організацій, які намагаються оголосити себе законодавцями в тій чи іншій області, хоча б «на годину».

Актуальність проблеми підкреслюється епічними інцидентами. Industroyer, BrickerBot, Mirai – і це лише видима верхівка айсберга, а що «день прийдешній нам готує»? Якщо продовжувати рухатися за течією, то господарями IoT стануть ботнети та інші «шкідники». А речі з непродуманим функціоналом будуть тяжіти над тими, хто спробує стати їх господарем. На рис.1.1 відображено проникнення IoT в в промисловість (industrial) та життя людей (consumer – споживач).

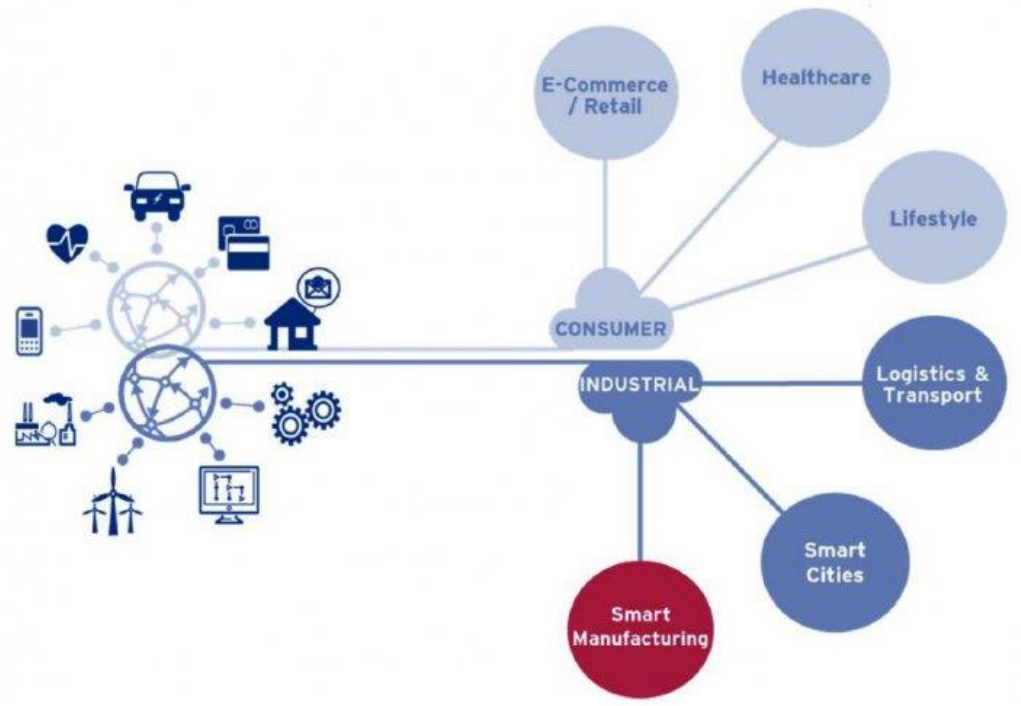

Рисунок 1.1 – Потужне проникнення IIoT в промисловість та в життя людей

У листопаді 2018 ENISA (The European Union Agency for Network and Information Security) випустило документ «Good Practices for Security of Internet of Things in the context of Smart Manufacturing», в якому зібрані всілякі практики забезпечення кібербезпеки для промислового IoT, причому проаналізовано близько сотні документів з кращими практиками в цій області. Що ж знаходиться «під капотом» цієї спроби осягнути неосяжне?

Промисловий IIoT (Industrial IoT), що включає, в тому числі, об'єкти критичної інформаційної інфраструктури, стоїть дещо окремо від класичного IoT .

Оператори IIoT систем звикли впроваджувати досить зрілі технічні рішення з горизонтом експлуатації в десятки років. Таким чином, впровадження модернізацій та інновацій з використанням IIoT рішень стримується динамічністю ринку з відсутністю загальноприйнятої системи стандартів і загальноприйнятих схем сертифікації.

Посилена оцифровка та зв’язок збільшують ризики кібербезпеки, роблячи таким чином суспільство в цілому більш вразливим до кіберзагроз та посилюючи небезпеку, з якою стикаються окремі особи, включаючи вразливі особи, такі як діти. Для пом'якшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки в Союзі, щоб мережеві та інформаційні системи, комунікаційні мережі, цифрові продукти, послуги та пристрої, що використовуються громадянами, організаціями та бізнесом, починаючи від малого та середнього підприємств (МСП), як визначено в Рекомендації Комісії 2003/361/ЄС [1], для операторів критичної інфраструктури - краще захищені від кіберзагроз.

Оприлюднюючи відповідну інформацію для громадськості, ENISA, засноване Регламентом (ЄС) No 526/2013 Європейського Парламенту та Ради [2], сприяє розвитку галузі кібербезпеки в Союзі, зокрема МСП та стартапи. ENISA повинна прагнути до більш тісної співпраці з університетами та дослідницькими структурами, щоб сприяти зменшенню залежності від продуктів та послуг кібербезпеки з-за меж Союзу та зміцненню ланцюгів поставок всередині Союзу.

Кібератаки збільшуються, і пов'язана економіка та суспільство, які є більш вразливими до кіберзагроз та атак, вимагають більш сильного захисту.

Однак, хоча кібератаки часто відбуваються через кордони, компетенція та відповідні заходи з боку кібербезпеки та правоохоронних органів є переважно національними.

Масштабні інциденти можуть порушити надання основних послуг по всьому Союзу. Це вимагає ефективних та скоординованих реакцій та врегулювання криз на рівні Союзу, спираючись на спеціальну політику та більш широкі інструменти європейської солідарності та взаємодопомоги.

Більше того, регулярна оцінка стану кібербезпеки та стійкості в Союзі на основі надійних даних Союзу, а також систематичних прогнозів майбутніх подій, викликів та загроз на рівні Союзу та на глобальному рівні є важливими для політиків, промисловості та користувачів.

У світлі посилених викликів кібербезпеки, з якими стикається Союз, існує потреба у всебічному наборі заходів, який би спирався на попередні дії Союзу та сприяв би взаємно підкріплюючим цілям.

Ці цілі включають подальше збільшення можливостей та готовності держав-членів та підприємств, а також покращення співпраці, обміну інформацією та координації між державами-членами та установами, органами, установами та установами Союзу.

Крім того, з огляду на безмежний характер кіберзагроз, існує потреба у збільшенні можливостей на рівні Союзу, які могли б доповнити дії держав-членів, зокрема у випадках масштабних транскордонних інцидентів та криз, при цьому враховуючи важливість підтримання та подальшого посилення національних можливостей реагувати на кіберзагрози будь-якого масштабу.

Також необхідні додаткові зусилля для підвищення обізнаності громадян, організацій та бізнесу з питань кібербезпеки. Більше того, враховуючи те, що інциденти підривають довіру до постачальників цифрових послуг та до самого єдиного цифрового ринку, особливо серед споживачів, довіру слід ще більше зміцнювати, пропонуючи прозорою інформацією про рівень безпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, що наголошує, що навіть високий рівень сертифікації кібербезпеки не може гарантувати, що продукт ІКТ, послуга ІКТ чи процес ІКТ є повністю безпечними. Збільшенню довіри може сприяти загальносоюзний сертифікат, що передбачає загальні вимоги щодо кібербезпеки та критерії оцінки на національних ринках та секторах.

Кібербезпека — це не лише питання, пов’язане з технологіями, але й те, де поведінка людини однаково важлива [3]. Отже, слід суворо заохочувати „кібергігієну”, а саме прості, рутинні заходи, які, коли громадяни, організації та підприємства здійснюють та проводять регулярно, мінімізують їх ризик від

кіберзагроз.

З метою посилення структур кібербезпеки Союзу важливо підтримувати та розвивати можливості держав-членів комплексно реагувати на кіберзагрози, включаючи транскордонні інциденти.

Підприємства та окремі споживачі повинні мати точну інформацію щодо рівня довіри, з яким сертифікована безпека їхніх продуктів ІКТ, послуг ІКТ та процесів ІКТ. У той же час жоден продукт ІКТ чи послуга ІКТ не є повністю кіберзахищеними, і основні правила кібергігієни повинні пропагуватися та визначатись за пріоритетами. З огляду на зростаючу доступність пристроїв IoT, існує низка добровільних заходів, які приватний сектор може вжити для зміцнення довіри до безпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ.

Сучасні ІКТ-продукти та системи часто інтегрують і покладаються на одну або кілька сторонніх технологій та компонентів, таких як програмні модулі, бібліотеки або інтерфейси прикладного програмування. Ця залежність, яку називають «залежністю», може створювати додаткові ризики кібербезпеки, оскільки уразливості, виявлені в сторонніх компонентах, можуть також впливати на безпеку продуктів ІКТ, послуг ІКТ та процесів ІКТ. У багатьох випадках виявлення та документування таких залежностей дозволяє кінцевим споживачам продуктів ІКТ, послуг ІКТ та процесів ІКТ покращувати свою діяльність з управління ризиками кібербезпеки, вдосконалюючи, наприклад, процедури управління уразливістю та виправлення вразливості користувачів.

Організації, виробники або постачальники, що беруть участь у проектуванні та розробці продуктів ІКТ, послуг ІКТ або процесах ІКТ, слід заохочувати до здійснення заходів на самих ранніх стадіях проектування та розробки для захисту безпеки цих продуктів, послуг та процесів у максимально можливій мірі , таким чином, що передбачається поява кібератак, а також передбачається та зводиться до мінімуму їх вплив («передбачена безпека»). Безпека повинна забезпечуватися протягом усього терміну експлуатації ІКТ-продукту, послуги ІКТ або процесу ІКТ шляхом проектування та розробки процесів, які постійно розвиваються, щоб зменшити ризик шкоди від зловмисної експлуатації.

Підприємства, організації та державний сектор повинні налаштовувати продукти ІКТ, послуги ІКТ або процеси ІКТ, розроблені ними, таким чином, щоб забезпечити більш високий рівень безпеки, який повинен дозволити першому користувачеві отримати конфігурацію за замовчуванням із максимально безпечними налаштуваннями (безпека за замовчуванням), тим самим зменшуючи навантаження на користувачів необхідністю налаштовувати продукт ІКТ, послугу ІКТ або процес ІКТ належним чином. Безпека за замовчуванням не повинна вимагати великої конфігурації або специфічного технічного розуміння або неінтуїтивної поведінки з боку користувача, а також повинна працювати легко та надійно при впровадженні. Якщо в кожному конкретному випадку аналіз ризику та зручності користування призводить до висновку, що такий параметр за замовчуванням неможливий, користувачам слід запропонувати вибрати найбільш безпечний параметр.

Регламент (ЄС) No 460/2004 Європейського Парламенту та Ради створив ENISA з метою сприяння досягненню цілей забезпечення високого та ефективного рівня мережевої та інформаційної безпеки в межах Союзу та розвитку культури мережева та інформаційна безпека на благо громадян, споживачів, підприємств та державних адміністрацій.

Регламент (ЄС) No 1007/2008 Європейського Парламенту та Ради продовжив мандат ENISA до березня 2012 року, регламент (ЄС) № 580/2011 Європейського Парламенту та Ради додатково продовжив мандат ENISA до 13 вересня 2013р., а регламент (ЄС) No 526/2013 продовжив мандат ENISA до 19 червня 2020р. [2].

1.2 Аналіз шляхів забезпечення кібербезпеки та підвищення довіри до цифрових технологій в ЄС

ЄС вже зробив важливі кроки для забезпечення кібербезпеки та підвищення довіри до цифрових технологій.

У 2013 році була прийнята Стратегія кібербезпеки Європейського Союзу,

яка спрямовувала політику реагування Союзу на кіберзагрози та ризики.

З метою кращого захисту громадян в Інтернеті, перший правовий акт Союзу в галузі кібербезпеки був прийнятий у 2016 році у формі Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради [4].

Директива (ЄС) 2016/1148 запровадила вимоги щодо національних можливостей у галузі кібербезпеки, встановила перші механізми для посилення стратегічного та оперативного співробітництва між державами-членами та запровадила зобов'язання щодо заходів безпеки та повідомлень про інциденти у секторах, що є життєво важливими економіка та суспільство, такі як енергетика, транспорт, постачання та розподіл питної води, банківська справа, інфраструктура фінансового ринку, охорона здоров’я, цифрова інфраструктура, а також ключові постачальники цифрових послуг (пошукові системи, послуги хмарних обчислень та онлайнові ринки).

ENISA була відведена ключова роль у підтримці імплементації цієї Директиви.

Крім того, ефективна боротьба з кіберзлочинністю стала важливим пріоритетом у Європейській програмі безпеки, сприяючи загальній меті досягнення високого рівня кібербезпеки. Інші правові акти, такі як Регламент (ЄС) 2016/679 Європейського Парламенту та Ради [5] та Директиви 2002/58/ЄС та (ЄС) 2018/1972 Європейського Парламенту та Ради також сприяють високому рівню кібербезпеки на єдиному цифровому ринку.

З моменту прийняття Стратегії кібербезпеки Європейського Союзу в 2013 році та останнього перегляду мандату ENISA загальний політичний контекст значно змінився, оскільки глобальне середовище стало більш невизначеним та менш безпечним.

На цьому тлі та в контексті позитивного розвитку ролі ENISA як орієнтира для консультацій та досвіду, як фасилітатора співпраці та розбудови спроможності, а також у рамках нової політики Союзу щодо кібербезпеки, необхідно переглянути мандат ENISA, встановити її роль в зміненій екосистемі кібербезпеки та забезпечити її ефективний внесок у відповідь Союзу на виклики

кібербезпеки, що випливають із кардинально трансформованого ландшафту кіберзагрози, для яких, як було визнано під час оцінки ENISA, поточного мандату недостатньо.

1.3 Аналіз завдань Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) в галузі кібербезпеки згідно Акту про кібербезпеку (Регламент ЄС 2019/881)

ENISA, встановлена Регламентом (ЄС) 2019/881 [3], оновлює ENISA, яка була встановлена Регламентом (ЄС) No 526/2013 [2]. ENISA повинна виконувати завдання, покладені на неї Регламентом (ЄС) 2019/881 та іншими нормативно-правовими актами Союзу в галузі кібербезпеки, серед іншого, надаючи консультації та досвід та виступаючи центром інформації та знань Союзу. Він повинен сприяти обміну найкращими практиками між державами-членами та приватними зацікавленими сторонами, пропонувати політичні пропозиції Комісії та державам-членам, виступати в якості орієнтира для галузевих політичних ініціатив Союзу щодо питань кібербезпеки та сприяти оперативній співпраці між державами-членами Державами та між державами-членами та установами, органами, установами та установами Союзу.

У рамках Рішення 2004/97/ЄС Є, прийнятого за спільною домовленістю між представниками держав-членів, проводить засідання на рівні глави держави або уряду, представники держав-членів вирішили, що ENISA матиме місце в місті в Греції, яке визначатиме грецький уряд.

Приймаюча держава-член ENISA повинна забезпечити найкращі можливі умови для безперебійної та ефективної роботи ENISA. Важливо для належного та ефективного виконання своїх завдань, для набору та утримання персоналу та для підвищення ефективності мережевої діяльності, щоб ENISA базувалась у відповідному місці, серед іншого забезпечуючи належне транспортне сполучення та умови для подружжя та дітей, що супроводжують членів співробітників ENISA. Необхідні заходи повинні бути викладені в угоді між ENISA та

приймаючою державою-членом, що укладається після отримання схвалення Правлінням ENISA.

З огляду на зростаючі ризики та виклики в галузі кібербезпеки, з якими стикається Союз, фінансові та людські ресурси, що виділяються ENISA, слід збільшити, щоб відобразити його посилену роль та завдання, а також його критичну позицію в екосистемі організацій, які захищають цифрову екосистему Союзу, що дозволить ENISA ефективно виконувати завдання, покладені на нього Регламентом (ЄС) 2019/881.

ENISA повинна:

а) розвивати та підтримувати високий рівень досвіду та діяти як орієнтир, встановлюючи довіру та впевненість у єдиному ринку в силу своєї незалежності, якості наданих консультацій, якості інформації, яку вона поширює, прозорості її процедур, прозорість методів його роботи та ретельність у виконанні своїх завдань;

б) активно підтримувати національні зусилля та повинна активно сприяти зусиллям Союзу, виконуючи свої завдання у повній співпраці з установами, органами, установами та установами Союзу та з державами-членами, уникаючи дублювання роботи та сприяючи взаємодії;

в) спиратись на внески та співпрацю з приватним сектором, а також іншими відповідними зацікавленими сторонами.

Для того, щоб мати змогу надати належну підтримку оперативній співпраці між державами-членами, ENISA повинна ще більше посилити свої технічні та людські можливості та навички. ENISA повинна збільшити свої ноу-хау та можливості. ENISA та держави-члени на добровільних засадах можуть розробляти програми для відрядження національних експертів до ENISA, створюючи пули обміну експертами та персоналом.

ENISA повинна:

а) допомагати Комісії шляхом надання порад, думок та аналізів щодо всіх питань Союзу, пов'язаних з розробкою політики та законодавства, оновлення та оглядів у галузі кібербезпеки та її секторальних аспектів, з метою підвищення

відповідності політики та законів Союзу вимір кібербезпеки та забезпечити послідовність у впровадженні цієї політики та законів на національному рівні;

б) виступати в якості орієнтира для отримання порад та досвіду для конкретних галузевих політичних та правових ініціатив Союзу, де беруть участь питання, пов'язані з кібербезпекою;

в) регулярно інформувати Європейський Парламент про свою діяльність.

Публічне ядро відкритого Інтернету, а саме його основні протоколи та інфраструктура, що є глобальним суспільним благом, забезпечує важливу функціональність Інтернету в цілому та підтримує його нормальну роботу. ENISA повинна підтримувати безпеку публічного ядра відкритого Інтернету та стабільність його функціонування, включаючи, але не обмежуючись цим, ключові протоколи (зокрема, DNS, BGP та IPv6), роботу системи доменних імен (таких як роботи всіх доменів верхнього рівня), а також роботи кореневої зони.

Основним завданням ENISA є сприяння послідовному впровадженню відповідної правової бази, зокрема ефективному впровадженню Директиви (ЄС) 2016/1148 [4] та інших відповідних правових інструментів, що містять аспекти кібербезпеки, що має важливе значення для підвищення стійкості до кібернетики. З огляду на швидко розвивається кіберзагрозу, очевидно, що держави-члени повинні бути підтримані більш всеосяжним крос-політичним підходом до формування кіберстійкості.

ENISA повинна допомагати державам-членам та установам, органам, управлінням та установам Союзу в їх зусиллях щодо нарощування та підвищення спроможності та готовності для запобігання, виявлення та реагування на кіберзагрози та інциденти та стосовно безпеки мережевих та інформаційних систем. Зокрема, ENISA повинна підтримувати розробку та вдосконалення національних та союзних груп реагування на випадки комп’ютерної безпеки (CSIRT), передбачених Директивою (ЄС) 2016/1148 [4], з метою досягнення високого загального рівня їх зрілості в Союзі. Діяльність, що проводиться ENISA щодо оперативних можливостей держав-членів, повинна активно підтримувати дії, вжиті державами-членами для виконання своїх зобов'язань за Директивою

(ЄС) 2016/1148, а отже, не повинна їх замінювати.

ENISA також повинна сприяти:

а) розробці та оновленню стратегій безпеки мережних та інформаційних систем на рівні Союзу та, за запитом, на рівні держав-членів, зокрема щодо кібербезпеки, а також повинна сприяти поширенню таких стратегій та стежити за прогресом їх здійснення;

б) покриттю потреби у навчанні та навчальних матеріалах, включаючи потреби державних органів, і, де це доречно, значною мірою "навчати інструкторів", спираючись на Цифрову систему компетентностей для громадян з метою надання допомоги членам Держави та установи, органи, установи та установи Союзу у розвитку власних навчальних можливостей.

ENISA повинна підтримувати держави-члени у сфері підвищення обізнаності та освіти щодо кібербезпеки, сприяючи більш тісній координації та обміну найкращими практиками між державами-членами. Така підтримка може полягати у розвитку мережі національних контактних пунктів освіти та розробці навчальної платформи з кібербезпеки. Мережа національних контактних пунктів освіти могла б діяти в рамках Національної мережі офіцерів зв’язку та бути відправною точкою для майбутньої координації в державах-членах.

ENISA повинна допомагати Групі співробітництва, створеній Директивою (ЄС) 2016/1148, у виконанні її завдань, зокрема шляхом надання експертних знань, порад та сприяння обміну найкращими практиками, зокрема, щодо визначення операторів основних послуги державами-членами, а також стосовно транскордонних залежностей щодо ризиків та інцидентів.

З метою стимулювання співпраці між державним та приватним сектором та всередині приватного сектору, зокрема для підтримки захисту критичних інфраструктур, ENISA повинна підтримувати обмін інформацією всередині та між секторами, зокрема секторами, переліченими у Додатку II до Директиви (ЄС) 2016/1148, надаючи найкращі практики та вказівки щодо доступних інструментів та процедур, а також надаючи вказівки щодо вирішення регуляторних питань, пов’язаних з обміном інформацією, наприклад, сприяючи створенню галузевих

центрів обміну інформацією та аналізу.

Тоді як потенційний негативний вплив вразливостей в продуктах ІКТ, послугах ІКТ та процесах ІКТ постійно збільшується, пошук та усунення таких вразливостей відіграє важливу роль у зменшенні загального ризику кібербезпеки. Доведено, що співпраця між організаціями, виробниками або постачальниками вразливих продуктів ІКТ, послуг ІКТ та процесів ІКТ, а також членами дослідницького співтовариства з питань кібербезпеки та урядами, які виявляють вразливі місця, суттєво збільшує швидкість виявлення та усунення вразливостей у продуктах ІКТ, ІКТ послуги та процеси ІКТ. Узгоджене розкриття вразливостей визначає структурований процес співпраці, в якому вразливості повідомляються власнику інформаційної системи, надання організації можливості діагностувати та усунути вразливість до розкриття детальної інформації про вразливість третім особам або громадськості. Процес також передбачає координацію між пошукачем та організацією щодо публікації цих вразливих місць. Узгоджена політика розкриття вразливості може зіграти важливу роль у зусиллях держав-членів щодо посилення кібербезпеки.

ENISA повинна узагальнювати та аналізувати загальнодоступні національні звіти CSIRT та міжвідомчої групи комп’ютерних команд реагування на надзвичайні ситуації для установ, органів та установ Союзу, створених домовленістю між Європейським Парламентом, Європейською Радою, Радою Європейського Союзу Комісія, Суд Європейського Союзу, Європейський центральний банк, Європейський аудиторський суд, Європейська служба зовнішніх дій, Європейський економічний та соціальний комітет, Європейський комітет регіонів та Європейський інвестиційний банк з питань організації та робота комп'ютерної групи реагування на надзвичайні ситуації для установ, органів та установ Союзу (CERT-EU) з метою сприяння встановленню загальних процедур, мови та термінології для обміну інформацією. У цьому контексті ENISA повинна залучати приватний сектор в рамках Директиви (ЄС) 2016/1148 [4], яка встановлює підстави для добровільного обміну технічною інформацією на оперативному рівні в мережі команд реагування на випадки комп’ютерної безпеки

(«мережа CSIRTs»), створені цією Директивою.

ENISA повинна сприяти реагуванню на рівні Союзу у випадку масштабних транскордонних інцидентів та криз, пов'язаних з кібербезпекою. Це завдання повинно виконуватися відповідно до мандата ENISA відповідно до Регламенту (ЄС) 2019/881 [3] та підходу, який узгоджується державами-членами в контексті Рекомендації Комісії (ЄС) 2017/1584 [6] та висновки Ради від 26 червня 2018 року щодо скоординованого реагування ЄС на масштабні інциденти та кризи в галузі кібербезпеки. Це завдання може включати збір відповідної інформації та виступати в ролі посередника між мережею CSIRT та технічним співтовариством, а також між особами, що приймають рішення, відповідальними за врегулювання криз. Крім того, ENISA повинна підтримувати оперативну співпрацю між державами-членами, за запитом однієї або декількох держав-членів, у вирішенні інцидентів з технічної точки зору, сприяючи відповідному обміну технічними рішеннями між державами-членами та забезпечуючи внесок у публічну комунікацію. ENISA повинна підтримувати оперативну співпрацю, перевіряючи механізми такої співпраці шляхом регулярних навчань з кібербезпеки.

Підтримуючи оперативну співпрацю, ENISA повинна використовувати наявний технічний та оперативний досвід CERT-EU через структуровану співпрацю. Така структурована співпраця може спиратися на досвід ENISA. Там, де це доцільно, слід укласти спеціальні домовленості між двома структурами для визначення практичного здійснення такої співпраці та уникнення дублювання діяльності.

Виконуючи своє завдання з підтримки оперативного співробітництва в мережі CSIRT, ENISA повинна мати можливість надавати підтримку державам-членам на їх прохання, наприклад, надаючи поради щодо того, як поліпшити їх можливості щодо запобігання, виявлення та реагування на інциденти, сприяючи технічна обробка інцидентів, що мають значний або суттєвий вплив, або забезпечення аналізу кіберзагроз та інцидентів. ENISA повинна сприяти технічному вирішенню інцидентів, що мають значний або суттєвий вплив, зокрема, підтримуючи добровільний обмін технічними рішеннями між

державами-членами або шляхом надання комбінованої технічної інформації, такої як технічні рішення, які добровільно надаються державами-членами. Рекомендація (ЄС) 2017/1584 [6] рекомендує державам-членам добросовісно співпрацювати та обмінюватися між собою та ENISA інформацією про масштабні інциденти та кризи, пов'язані з кібербезпекою, без зайвої затримки. Така інформація додатково допоможе ENISA у виконанні її завдання з підтримки оперативного співробітництва.

В рамках регулярної співпраці на технічному рівні з метою забезпечення обізнаності про ситуацію в Союзі, ENISA, у тісній співпраці з державами-членами, повинна підготувати регулярний поглиблений звіт про технічну ситуацію з питань кібербезпеки ЄС щодо інцидентів та кіберзагроз на основі загальнодоступної інформації, власний аналіз та звіти, якими обмінюються з ними CSIRT держав-членів або національні єдині контактні пункти щодо безпеки мережі та інформаційних систем («єдині контактні пункти»), передбачені Директивою (ЄС) 2016/1148 [4], як щодо добровільної Європейський центр з кіберзлочинності (EC3) при Європолі, CERT-EU та, де це доречно, Центр розвідки та ситуації Європейського Союзу (EU INTCEN) при Європейській службі зовнішніх дій. Цей звіт повинен бути наданий Раді, Комісії, Верховному представнику Союзу із закордонних справ та політики безпеки та мережі CSIRT (Computer security incident response team).

Підтримка ENISA для колишнього поста технічного розслідування інцидентів, що мають значну або суттєвий вплив, проведеного на прохання зацікавлених держав-членів повинні бути направлено на запобігання майбутніх інцидентів. Зацікавлені держави-члени повинні надавати необхідну інформацію і допомогу, з тим щоб ENISA підтримати екс-пост ефективного технічного розслідування.

Держави-члени можуть запросити підприємства, яких стосується інцидент, до співпраці, надаючи необхідну інформацію та допомогу ENISA без шкоди для їх права на захист комерційно конфіденційної інформації та інформації, яка має відношення до громадської безпеки.

Для кращого розуміння викликів у галузі кібербезпеки та з метою надання стратегічних довгострокових порад державам-членам та установам, органам, бюро та агентствам Союзу, ENISA має проаналізувати поточні та нові ризики кібербезпеки. З цією метою ENISA повинна у співпраці з державами-членами та, за необхідності, зі статистичними органами та іншими органами, збирати відповідну загальнодоступну або добровільно надану інформацію та проводити аналіз нових технологій та надавати конкретні оцінки щодо очікуваних соціальних, правових, економічний та регулятивний вплив технологічних інновацій на мережеву та інформаційну безпеку, зокрема кібербезпеку. Крім того, ENISA повинна підтримувати держави-члени та установи, органи, установи та установи Союзу у виявленні нових ризиків кібербезпеки та запобіганні інцидентам шляхом проведення аналізу кіберзагроз, вразливостей та інцидентів.

З метою підвищення стійкості Союзу ENISA повинна розвивати досвід у галузі кібербезпеки інфраструктур, зокрема для підтримки секторів, перелічених у Додатку II до Директиви (ЄС) 2016/1148, та тих, що використовуються постачальниками цифрових послуг. перелічені у Додатку III до цієї Директиви, надаючи поради, видаючи настанови та обмінюючись найкращими практиками. З метою забезпечення спрощеного доступу до більш структурованої інформації про ризики кібербезпеки та можливі засоби правового захисту, ENISA повинна розробити та підтримувати «інформаційний центр» Союзу - єдиний портал, що надає громадськості інформацію про кібербезпеку, що походить із Союзу та національні установи, органи, бюро та агентства.

ENISA повинна:

а) сприяти підвищенню обізнаності громадськості про ризики кібербезпеки, в тому числі за допомогою загальноєвропейської кампанії підвищення рівня обізнаності шляхом сприяння освіті та надання вказівок щодо передових практик для окремих користувачів, спрямованих на громадян, організації та бізнес;

б) сприяти просуванню найкращих практик та рішень, включаючи кібергігієну та кіберграмотність на рівні громадян, організацій та підприємств,

збираючи та аналізуючи загальнодоступну інформацію про значні інциденти, а також складаючи та публікуючи звіти та вказівки для громадян, організацій та підприємств, щоб підвищити загальний рівень готовності та стійкості;

в) прагнути надавати споживачам відповідну інформацію про придатні схеми сертифікації, наприклад, шляхом надання вказівок та рекомендацій;

г) організувати, відповідно до Плану дій щодо цифрової освіти, встановленого у Повідомленні Комісії від 17 січня 2018 року, та у співпраці з державами-членами та установами, органами, установами та установами Союзу регулярні інформаційно-просвітницькі та громадські освітні кампанії, спрямовані на кінцевих користувачів, з метою сприяти безпечнішій поведінці в Інтернеті приватних осіб та цифровій грамотності, підвищувати обізнаність про потенційні кіберзагрози, включаючи злочинні дії в Інтернеті, такі як фішинг-атаки, ботнети, фінансові та банківські шахрайства, випадки шахрайства з даними, та сприяти базовій багатофакторній автентифікації, виправленню, шифруванню, поради щодо анонімізації та захисту даних.

ENISA повинна відігравати центральну роль у пришвидшенні обізнаності кінцевих користувачів про безпеку пристроїв та безпечне користування послугами, а також повинна сприяти розробці безпеки та конфіденційності на рівні Союзу. Для досягнення цієї мети ENISA повинна використовувати наявні найкращі практики та досвід, особливо найкращі практики та досвід академічних установ та дослідників ІТ-безпеки.

Для підтримки підприємств, що працюють у секторі кібербезпеки, а також користувачів рішень з кібербезпеки, ENISA повинна розробити та підтримувати «обсерваторію ринку», проводячи регулярні аналізи та розповсюджуючи інформацію про основні тенденції на ринку кібербезпеки, як сторони попиту та пропозиції.

ENISA повинна сприяти зусиллям Союзу щодо співпраці з міжнародними організаціями, а також у рамках відповідних рамок міжнародного співробітництва у галузі кібербезпеки. Зокрема, ENISA повинна сприяти, де це доречно, співпраці з такими організаціями, як ОЕСР, ОБСЄ та НАТО. Така співпраця може включати

спільні навчання з кібербезпеки та спільну координацію реагування на інциденти. Ці заходи повинні здійснюватися з повною дотриманням принципів інклюзивності, взаємності та автономності прийняття рішень Союзу, без шкоди для специфічного характеру політики безпеки та оборони будь-якої держави-члена.

ENISA також повинна взаємодіяти з органами влади, які займаються захистом даних, з метою обміну ноу-хау та найкращими практиками, а також повинна надавати поради щодо питань кібербезпеки, які можуть вплинути на їх роботу. Представники національних та союзних правоохоронних органів та органів захисту даних повинні мати право бути представленими в Консультативній групі ENISA. Спілкуючись із правоохоронними органами щодо питань мережевої та інформаційної безпеки, які можуть вплинути на їх роботу, ENISA повинна поважати існуючі канали інформації та створені мережі. Представники національних та союзних правоохоронних органів та органів захисту даних повинні мати право бути представленими в Консультативній групі ENISA. Спілкуючись із правоохоронними органами щодо питань мережевої та інформаційної безпеки, які можуть вплинути на їх роботу, ENISA повинна поважати існуючі канали інформації та створені мережі. Представники національних та союзних правоохоронних органів та органів захисту даних повинні мати право бути представленими в Консультативній групі ENISA. Спілкуючись із правоохоронними органами щодо питань мережевої та інформаційної безпеки, які можуть вплинути на їх роботу, ENISA повинна поважати існуючі канали інформації та створені мережі.

Можна встановити партнерські стосунки з академічними установами, які проводять дослідницькі ініціативи у відповідних галузях, і повинні існувати відповідні канали для участі споживчих організацій та інших організацій, що слід враховувати.

ENISA, виконуючи роль секретаріату мережі CSIRT, повинна підтримувати CSIRT держав-членів та CERT-EU в оперативному співробітництві щодо відповідних завдань мережі CSIRT, як зазначено в Директиві (ЄС) 2016/1148 [4].

Крім того, ENISA повинна сприяти та підтримувати співпрацю між відповідними CSIRT у випадку інцидентів, атак або збоїв у роботі мереж або інфраструктури, що управляються або захищаються CSIRT, і залучають або можуть залучати принаймні два CSIRT, беручи до уваги Стандартну операційну діяльність Процедури мережі CSIRT.

З метою підвищення готовності Союзу реагувати на інциденти, ENISA повинна регулярно організовувати навчання з кібербезпеки на рівні Союзу та, на їх прохання, підтримувати держави-члени та установи, органи, установи та установи Союзу в організації таких навчань. Масштабні комплексні навчання, які включають технічні, оперативні або стратегічні елементи, повинні організовуватися раз на два роки. Крім того, ENISA повинна мати можливість регулярно організовувати менш комплексні навчання з тією ж метою підвищення готовності Союзу до реагування на інциденти.

ENISA повинна:

а) продовжувати розвивати та підтримувати свій досвід у галузі сертифікації кібербезпеки з метою підтримки політики Союзу в цій галузі;

б) спиратися на існуючі найкращі практики та повинна сприяти впровадженню сертифікації кібербезпеки в межах Союзу, в тому числі шляхом сприяння створенню та підтримці системи сертифікації кібербезпеки на рівні Союзу (європейська система сертифікації кібербезпеки) з метою підвищення прозорості забезпечення кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, тим самим зміцнюючи довіру до внутрішнього цифрового ринку та його конкурентоспроможності.

Ефективна політика кібербезпеки повинна базуватися на добре розроблених методах оцінки ризиків як у державному, так і в приватному секторах. Методи оцінки ризику використовуються на різних рівнях, і немає загальної практики щодо того, як їх ефективно застосовувати. Популяризація та розвиток найкращих практик оцінки ризиків та оперативно сумісних рішень щодо управління ризиками в державному та приватному секторах підвищить рівень кібербезпеки в Союзі. З цією метою ENISA повинна підтримувати співпрацю між зацікавленими

сторонами на рівні Союзу та сприяти їхнім зусиллям щодо встановлення та впровадження європейських та міжнародних стандартів управління ризиками та вимірюваної безпеки електронних продуктів, систем, мереж та послуг, які разом з програмним забезпеченням, включають мережу та інформаційні системи.

ENISA повинна заохочувати держави-члени, виробників чи постачальників продуктів ІКТ, послуг ІКТ чи процесів ІКТ підвищувати свої загальні стандарти безпеки, щоб усі користувачі Інтернету могли вжити необхідних заходів для забезпечення власної особистої кібербезпеки та повинні стимулювати це робити. Зокрема, виробники та постачальники ІКТ-продуктів, ІКТ-послуг чи ІКТ-процесів повинні надавати будь-які необхідні оновлення та відкликати, вилучати або переробляти ІКТ-продукти, ІКТ-послуги чи ІКТ-процеси, що не відповідають стандартам кібербезпеки, тоді як імпортери та дистриб'ютори повинні переконатися, що продукти ІКТ, послуги ІКТ та процеси ІКТ, які вони розміщують на ринку Союзу, відповідають чинним вимогам і не представляють ризику для споживачів Союзу.

Співпрацюючи з компетентними органами, ENISA повинна мати можливість поширювати інформацію щодо рівня кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, що пропонуються на внутрішньому ринку, і повинна видавати попередження для виробників або постачальників продуктів ІКТ, послуг ІКТ або ІКТ-процеси та вимагання від них покращення безпеки своїх ІКТ-продуктів, послуг ІКТ та ІКТ-процесів, включаючи кібербезпеку.

ENISA повинна повною мірою брати до уваги поточні дослідження, розробку та оцінку технологічної діяльності, зокрема ті заходи, що проводяться різними дослідницькими ініціативами Союзу, щоб консультувати установи, органи, установи та установи Союзу та, за необхідності, держави-члени на їх прохання щодо дослідницькі потреби та пріоритети у галузі кібербезпеки. Для того, щоб визначити потреби та пріоритети досліджень, ENISA також повинна проконсультуватися з відповідними групами користувачів. Більш конкретно, може бути створена співпраця з Європейською дослідницькою радою, Європейським інститутом інновацій та технологій та Інститутом досліджень

безпеки Європейського Союзу.

ENISA повинна регулярно консультуватися з організаціями стандартизації, зокрема європейськими організаціями стандартизації, під час підготовки європейських схем сертифікації кібербезпеки.

Кіберзагрози – глобальна проблема. Існує потреба у більш тісному міжнародному співробітництві для вдосконалення стандартів кібербезпеки, включаючи необхідність у визначенні загальних норм поведінки, прийнятті кодексів поведінки, використанні міжнародних стандартів та обміні інформацією, сприянні швидшому міжнародному співробітництву у відповідь на мережеві та питань інформаційної безпеки та просування спільного глобального підходу до таких питань. З цією метою ENISA повинна підтримувати подальше залучення Союзу та співпрацю з третіми країнами та міжнародними організаціями, надаючи необхідні знання та аналіз відповідним установам, органам, бюро та агентствам Союзу, де це доречно.

ENISA повинна мати можливість відповідати на спеціальні запити держав-членів та установ, органів, управлінь та установ Союзу щодо питань, що належать до повноважень ENISA.

Розумно та рекомендується впроваджувати певні принципи щодо управління ENISA з метою дотримання Спільної заяви та Спільного підходу, узгоджених у липні 2012 року Міжвідомчою робочою групою з питань децентралізованих установ ЄС, метою якої є впорядкування діяльність децентралізованих агентств та покращення їх роботи. Рекомендації у Спільній заяві та Спільному підході також повинні бути відображені, у відповідних випадках, у робочих програмах ENISA, оцінках ENISA та звітній та адміністративній практиці ENISA.

Для ефективної діяльності ENISA чималу роль відіграє те, наскільки грамотно організована її структура – чи немає непотрібних елементів або, навпаки, можливо якійсь частині агентству не вистачає? Тому, в цій роботі аналізується структура ENISA, яка показана на рис. 1.2.

Правління, до складу якого входять представники держав-членів та Комісії,

повинно встановити загальний напрямок діяльності ENISA та забезпечити виконання своїх завдань відповідно до Регламенту (ЄС) 2019/881 [3].

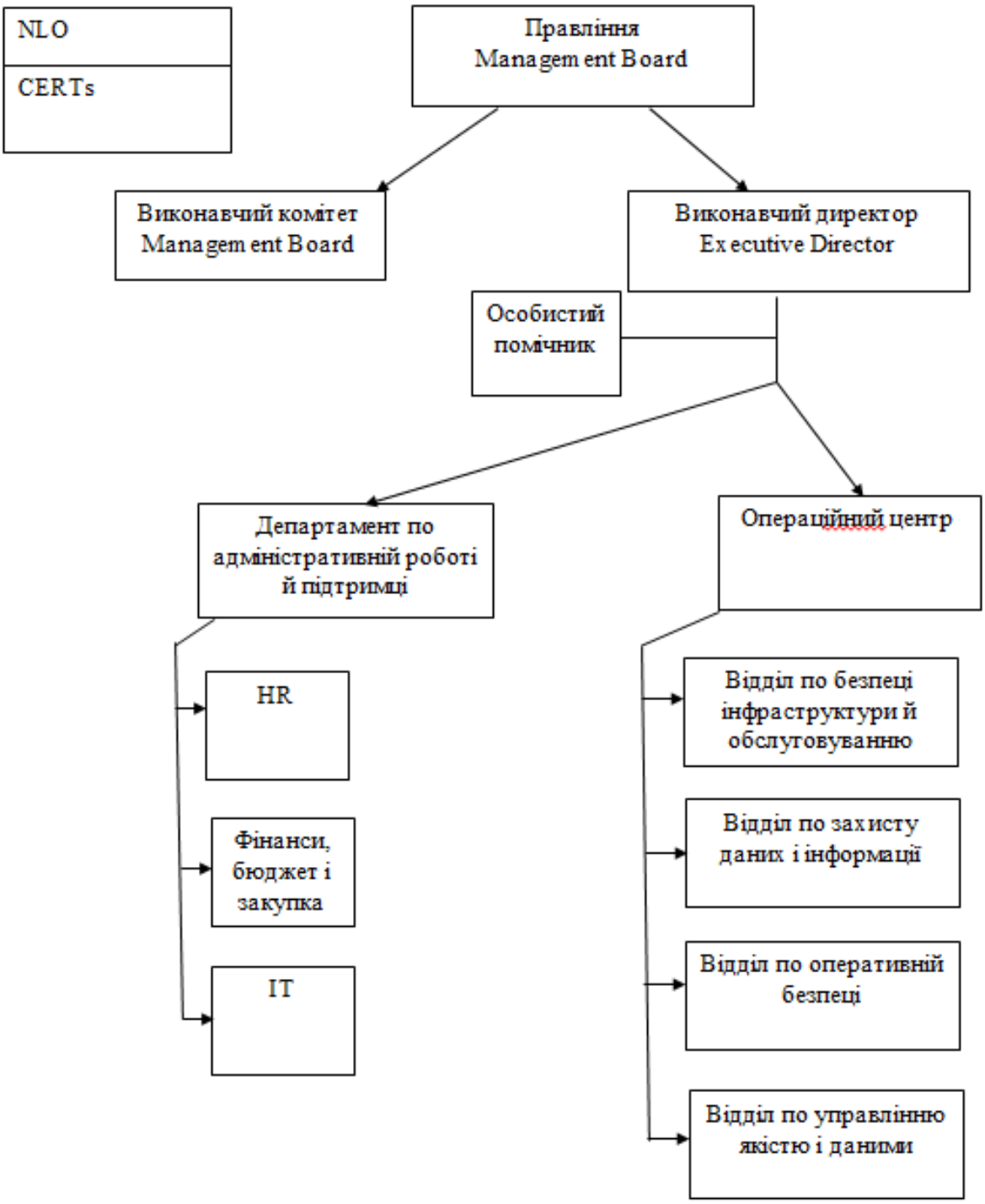

Рисунок 1.2 – Структура ENISA

Правлінню слід доручити повноваження, необхідні для формування бюджету, перевірки виконання бюджету, прийняття відповідних фінансових правил, встановлення прозорих робочих процедур для прийняття рішень ENISA, прийняття єдиного програмного документа ENISA, прийняття власних правил процедури, призначити виконавчого директора та прийняти рішення про продовження та припинення повноважень виконавчого директора.

Для того, щоб ENISA функціонувала належним чином та ефективно, Комісія та держави-члени повинні забезпечити, щоб особи, які призначаються до Правління, мали відповідний професійний досвід та досвід. Комісія та держави-члени також повинні докласти зусиль для обмеження обороту їх відповідних представників у Правлінні Раді, щоб забезпечити безперервність її роботи.

Безперебійне функціонування ENISA вимагає, щоб її виконавчий директор призначався на підставі заслуг та задокументованих адміністративних та управлінських навичок, а також компетентності та досвіду, що стосуються кібербезпеки. Обов'язки виконавчого директора повинні виконуватися з повною незалежністю. Виконавчий директор повинен підготувати пропозицію щодо річної робочої програми ENISA після попередньої консультації з Комісією та вжити всіх необхідних заходів для забезпечення належного виконання цієї робочої програми. Виконавчий директор повинен підготувати щорічний звіт, який буде подано до Правління, що охоплює виконання річної робочої програми ENISA, скласти проект звіту про кошториси доходів та витрат для ENISA та виконати бюджет.

Крім того, виконавчий директор повинен мати можливість створювати спеціальні робочі групи для вирішення конкретних питань, зокрема питань наукового, технічного, правового або соціально-економічного характеру. Зокрема, стосовно підготовки конкретної європейської схеми сертифікації кібербезпеки („схема кандидата”), створення спеціальної робочої групи вважається необхідним. Виконавчий директор повинен забезпечити, щоб члени спеціальних робочих груп були обрані відповідно до найвищих стандартів експертизи, що має на меті забезпечити гендерний баланс та відповідний баланс, відповідно до конкретних

питань, між державними адміністраціями держав-членів, установи, органи, бюро та агентства Союзу та приватний сектор, включаючи промисловість, користувачів та академічних експертів у галузі мережевої та інформаційної безпеки.

Виконавча рада повинна сприяти ефективному функціонуванню правління. В рамках своєї підготовчої роботи, пов'язаної з рішеннями Правління, Виконавча рада повинна детально вивчити відповідну інформацію, вивчити наявні варіанти та запропонувати поради та рішення для підготовки рішень Правління.

ENISA повинна мати консультативну групу ENISA як дорадчий орган для забезпечення регулярного діалогу з приватним сектором, організаціями споживачів та іншими відповідними зацікавленими сторонами. Консультативна група ENISA, створена Правлінням за пропозицією виконавчого директора, повинна зосередитись на питаннях, що мають значення для зацікавлених сторін, і повинна довести їх до відома ENISA. До консультативної групи ENISA слід звертатися, зокрема, щодо проекту річної програми роботи ENISA. Склад Консультативної групи ENISA та покладені на неї завдання повинні забезпечити достатнє представництво зацікавлених сторін у роботі ENISA.

Слід створити Групу з сертифікації кібербезпеки зацікавлених сторін, щоб допомогти ENISA та Комісії полегшити консультації з відповідними зацікавленими сторонами.

Група з сертифікації кібербезпеки зацікавлених сторін повинна складатися з членів, що представляють галузь у збалансованих пропорціях

а) як з боку попиту;

б) так і з боку пропозиції продуктів ІКТ та послуг ІКТ;

в) а також, зокрема:

1) МСП;

2) постачальників цифрових послуг;

3) європейських та міжнародних органів стандартизації;

4) національні органи з акредитації;

5) органи нагляду за захистом даних;

6) органи з оцінки відповідності (ООВ) відповідно до Регламенту

(ЄС) No 765/2008 Європейського Парламенту та Ради [7];

7) наукові кола;

8) організації споживачів.

На допомогу роботі ENISA також існує мережа національних співробітників по зв'язку NLO (National Liaison Officers network) по одному від кожної держави-члена Європейського союзу, Європейської асоціації Вільної торгівлі, Європейської комісії та Ради Європейського союзу. Дана мережа не базується на основі ENISA, але має велике значення для агентства, так як допомагає підтримувати тісний контакт з державами-членами ЄС, і підсилює тим самим роботу агентства в даних державах.

Ключовим інструментом для для захисту інформаційних інфраструктур критичної значущості є CERT (Computer Emergency Response Teams) – Команди Реагування на Комп'ютерні Надзвичайні ситуації. Дані команди існують в державі ЄС і покликані бути основним постачальником послуг безпеки для держави і громадян, а також займатися просвітницькою діяльністю. Однак не всі держави мають такою командою, тому місія ENISA забезпечити їх даними органом – в країнах Європи і за її межами. Крім того, ENISA знаходиться в постійній взаємодії з усіма CERTs. У майбутні плани агентства входить далі підтримувати створення подібних органів, створювати звіти про передовий досвід в сфері кіберінцидентів за допомогою CERTs, радити державам-членам ЄС у поліпшенні IT інфраструктури, а також тестувати CERTs.

ENISA повинна мати діючі правила щодо запобігання та управління конфліктом інтересів. ENISA також повинна застосовувати відповідні положення Союзу щодо доступу громадськості до документів, як зазначено в Регламенті (ЄС) № 1049/2001 Європейського Парламенту та Ради. Обробка персональних даних ENISA повинна регулюватися Регламентом (ЄС) 2018/1725 Європейського Парламенту та Ради. ENISA повинна дотримуватись положень, що застосовуються до установ, органів, бюро та агентств Союзу, а також національного законодавства щодо обробки інформації, зокрема конфіденційної некласифікованої інформації та секретної інформації ЄС (EUCI).

Для того, щоб гарантувати повну автономію та незалежність ENISA та дати їй змогу виконувати додаткові завдання, включаючи непередбачувані надзвичайні завдання, ENISA повинен отримувати достатній та автономний бюджет, доходи якого в першу чергу повинні надходити від внесків Союзу та внесків третіх країн участь у роботі ENISA. Відповідний бюджет є головним для забезпечення того, щоб ENISA мала достатній потенціал для виконання всіх своїх зростаючих завдань та досягнення своїх цілей. Більшість співробітників ENISA повинні брати безпосередню участь в оперативному виконанні мандата ENISA. Державі-члену, що приймає, та будь-якій іншій державі-члену має бути дозволено робити добровільні внески до бюджету ENISA. Бюджетна процедура Союзу повинна залишатися застосовною щодо будь-яких субсидій, що підлягають сплаті до загального бюджету Союзу. Більше того, Аудиторський суд повинен проводити аудит рахунків ENISA для забезпечення прозорості та підзвітності.

1.4 Дослідження ролі Європейської системи сертифікації кібербезпеки у підвищенні довіри та безпеки до інформаційних та телекомунікаційних технологій

Сертифікація кібербезпеки відіграє важливу роль у підвищенні довіри та безпеки до продуктів ІКТ, послуг ІКТ та процесів ІКТ.

Єдиний цифровий ринок, зокрема економіка даних та IoT, можуть процвітати лише за умови довіри загальної громадськості, що такі продукти, послуги та процеси забезпечують певний рівень кібербезпеки.

Підключені та автоматизовані машини, електронні медичні прилади, системи управління промисловою автоматизацією та інтелектуальні мережі - лише деякі приклади секторів, в яких сертифікація вже широко використовується або, можливо, буде використана найближчим часом.

Сектори, регульовані Директивою (ЄС) 2016/1148 [4], також є секторами, в яких сертифікація кібербезпеки є критично важливою.

У повідомленні 2016 року «Зміцнення європейської системи стійкості до

кіберпромисловості та сприяння розвитку конкурентоспроможної та інноваційної галузі кібербезпеки» Комісія зазначила потребу у високоякісних, доступних за ціною та сумісних продуктах та рішеннях для кібербезпеки.

Постачання ІКТ-продуктів, ІКТ-послуг та ІКТ-процесів на єдиному ринку залишається дуже фрагментованим у географічному плані. Це пов'язано з тим, що галузь кібербезпеки в Європі розвинулась здебільшого на основі національного державного попиту.

Крім того, відсутність сумісних рішень (технічних стандартів), практики та загальносоюзних механізмів сертифікації є серед інших прогалин, що впливають на єдиний ринок у галузі кібербезпеки.

Це ускладнює європейський бізнес конкуренцію на національному, союзному та глобальному рівнях. Це також зменшує вибір життєздатних та придатних до використання технологій кібербезпеки, до яких мають доступ фізичні та юридичні особи.

Подібним чином, у повідомленні 2017 року про середньостроковий огляд щодо впровадження стратегії єдиного цифрового ринку - підключений єдиний цифровий ринок для всіх, Комісія наголосила на необхідності безпечних підключених продуктів та систем та зазначила, що створення Європейської Правила безпеки ІКТ, що встановлюють правила організації сертифікації безпеки ІКТ у Союзі, можуть як зберегти довіру до Інтернету, так і подолати поточну фрагментацію внутрішнього ринку.

В даний час сертифікація кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ використовується лише обмежено.

Коли вона існує, це здебільшого відбувається на рівні держав-членів або в рамках галузевих схем.

У цьому контексті сертифікат, виданий національним органом з сертифікації кібербезпеки, в принципі не визнається в інших державах-членах.

Таким чином, компаніям, можливо, доведеться сертифікувати свої ІКТ-продукти, послуги ІКТ та процеси ІКТ у декількох державах-членах, де вони працюють, наприклад, з метою участі у національних процедурах закупівель, що

тим самим збільшує їх витрати. Більше того, поки з'являються нові схеми, схоже, не існує узгодженого та цілісного підходу до питань горизонтальної кібербезпеки, наприклад, у сфері IoT.

Деякі зусилля було докладено для того, щоб забезпечити взаємне визнання сертифікатів в межах Союзу. Однак вони досягли успіху лише частково. Найважливішим прикладом у цьому відношенні є Угода про взаємне визнання (MRA) групи вищих посадових осіб - Захист інформаційних систем (SOG-IS).

Хоча це найважливіша модель співпраці та взаємного визнання в галузі сертифікації безпеки, SOG-IS включає лише деякі держави-члени. Цей факт обмежив ефективність SOG-IS MRA з точки зору внутрішнього ринку.

Тому необхідно прийняти спільний підхід та створити європейську систему сертифікації кібербезпеки, яка встановлює основні горизонтальні вимоги до європейських схем сертифікації кібербезпеки та дозволяє європейським сертифікатам кібербезпеки та заявам ЄС про відповідність продукції ІКТ, послуг ІКТ або Процеси ІКТ повинні бути визнані та використані у всіх державах-членах.

Роблячи це, важливо спиратися на існуючі національні та міжнародні схеми, а також на системи взаємного визнання, зокрема SOG-IS, і забезпечити плавний перехід від існуючих схем за таких систем до схем за новою європейською система сертифікації кібербезпеки.

Європейська система сертифікації кібербезпеки повинна мати подвійне призначення.

По-перше, це повинно сприяти збільшенню довіри до продуктів ІКТ, Послуги ІКТ та процеси ІКТ, сертифіковані за європейськими схемами сертифікації кібербезпеки.

По-друге, це повинно допомогти уникнути множення суперечливих або дублюючих національних схем сертифікації кібербезпеки і тим самим зменшити витрати для підприємств, що працюють на єдиному цифровому ринку. Європейські схеми сертифікації кібербезпеки повинні бути недискримінаційними і базуватися на європейських або міжнародних стандартах, якщо тільки ці стандарти не є неефективними або невідповідними для виконання законних цілей

Союзу в цьому відношенні.

Європейська система сертифікації кібербезпеки повинна бути встановлена єдиним чином у всіх державах-членах, щоб запобігти "сертифікаційним покупкам", заснованим на різних рівнях жорсткості в різних державах-членах.

Європейські схеми сертифікації кібербезпеки повинні будуватися на основі того, що вже існує на міжнародному та національному рівнях, а при необхідності - на технічних специфікаціях форумів та консорціумів, вивченні поточних сильних сторін та оцінці та виправленні слабких сторін.

Гнучкі рішення з питань кібербезпеки необхідні для того, щоб галузь випереджала кіберзагрози, і тому будь-яка схема сертифікації повинна бути розроблена таким чином, щоб уникнути ризику швидко застаріти.

Комісія повинна бути уповноважена приймати європейські схеми сертифікації кібербезпеки стосовно конкретних груп продуктів ІКТ, послуг ІКТ та процесів ІКТ. Ці схеми повинні впроваджуватися і контролюватися національними органами з сертифікації кібербезпеки, а сертифікати, видані за цими схемами, повинні бути дійсними та визнаними в усьому Союзі. Схеми сертифікації, що експлуатуються галуззю або іншими приватними організаціями, повинні виходити за межі сфери дії Регламенту (ЄС) 2019/881 [3]. Однак органи, що експлуатують такі схеми, повинні мати можливість запропонувати Комісії розглядати такі схеми як основу для затвердження їх як європейської схеми сертифікації кібербезпеки.

Положення Регламенту (ЄС) 2019/881 не повинні шкодити законодавству Союзу, яке передбачає конкретні правила щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ. Зокрема, Регламент (ЄС) 2016/679 [5] встановлює положення щодо встановлення механізмів сертифікації та печаток та знаків захисту даних з метою демонстрації відповідності операцій обробки контролерами та процесорами цьому Регламенту. Такі механізми сертифікації та печатки та знаки захисту даних повинні дозволяти суб'єктам даних швидко оцінювати рівень захисту даних відповідних продуктів ІКТ, послуг ІКТ та процесів ІКТ. Цей Регламент не шкодить сертифікації операцій з обробки даних

відповідно до Регламенту (ЄС) 2016/679 [5], в тому числі, коли такі операції вбудовані в продукти ІКТ, послуги ІКТ та процеси ІКТ.

Метою європейських схем сертифікації кібербезпеки має бути забезпечення того, щоб продукція ІКТ, послуги ІКТ та процеси ІКТ, сертифіковані за такими схемами, відповідали визначеним вимогам, спрямованим на захист доступності, автентичності, цілісності та конфіденційності даних, що зберігаються, передаються або обробляються. пов'язані функції або послуги, що пропонуються або доступні через ці продукти, послуги та процеси протягом їх життєвого циклу.

У цьому Регламенті неможливо детально викласти вимоги до кібербезпеки, що стосуються всіх продуктів ІКТ, послуг ІКТ та процесів ІКТ.

Продукти ІКТ, послуги ІКТ та процеси ІКТ, а також потреби в кібербезпеці, пов’язані з цими продуктами, послугами та процесами, настільки різноманітні, що дуже складно розробити загальні вимоги до кібербезпеки, які діють за будь-яких обставин. Тому для цілей сертифікації необхідно прийняти широке та загальне поняття кібербезпеки, яке повинно доповнюватися набором конкретних цілей кібербезпеки, які слід враховувати при розробці європейських схем сертифікації кібербезпеки.

Домовленості, за допомогою яких такі цілі повинні бути досягнуті в конкретних продуктах ІКТ, послугах ІКТ та процесах ІКТ, повинні бути детально визначені на рівні індивідуальної схеми сертифікації, прийнятої Комісією, наприклад, посиланням на стандарти або технічні специфікації, якщо відповідні стандарти відсутні, що має доповнюватися набором конкретних цілей кібербезпеки, які слід враховувати при розробці європейських схем сертифікації кібербезпеки.

Технічні специфікації, які будуть використовуватися в європейських схемах сертифікації кібербезпеки, повинні відповідати вимогам, викладеним у Додатку II до Регламенту (ЄС) No 1025/2012 Європейського Парламенту та Ради [8]. Однак деякі відхилення від цих вимог можна вважати необхідними у належним чином обґрунтованих випадках, коли ці технічні специфікації повинні використовуватися в європейській схемі сертифікації кібербезпеки, що стосується

рівня довіри "високий". Причини таких відхилень повинні бути загальнодоступними.

Оцінка відповідності - це процедура оцінки того, чи були виконані визначені вимоги, що стосуються продукту ІКТ, послуги ІКТ чи процесу ІКТ [3]. Ця процедура здійснюється незалежною третьою стороною, яка не є виробником або постачальником продуктів ІКТ, послуг ІКТ чи процесів ІКТ, які оцінюються.

Європейський сертифікат кібербезпеки повинен видаватися після успішної оцінки продукту ІКТ, послуги ІКТ або процесу ІКТ.

Європейський сертифікат кібербезпеки слід вважати підтвердженням того, що оцінка була проведена належним чином. Залежно від рівня довіри, європейська схема сертифікації кібербезпеки повинна вказувати, чи слід видавати європейський сертифікат кібербезпеки приватним чи державним органом.

Оцінка відповідності та сертифікація самі по собі не можуть гарантувати, що сертифіковані продукти ІКТ, послуги ІКТ та процеси ІКТ є кібербезпечними. Натомість вони є процедурами та технічними методологіями для підтвердження того, що продукти ІКТ, послуги ІКТ та процеси ІКТ перевірені та відповідають певним вимогам кібербезпеки, викладеним в інших місцях, наприклад, у технічних стандартах.

Вибір відповідної сертифікації та відповідних вимог безпеки користувачами європейських сертифікатів кібербезпеки повинен базуватися на аналізі ризиків, пов'язаних із використанням продуктів ІКТ, послуг ІКТ чи процесів ІКТ. Відповідно, рівень довіри повинен бути співмірним із рівнем ризику, пов'язаного із передбачуваним використанням продукту ІКТ, послуги ІКТ або процесу ІКТ.

Європейські схеми сертифікації кібербезпеки можуть передбачати проведення оцінки відповідності під виключною відповідальністю виробника або постачальника продуктів ІКТ, послуг ІКТ або процесів ІКТ («самооцінка відповідності»). У таких випадках має бути достатньо, щоб виробник або постачальник продуктів ІКТ, послуг ІКТ або процесів ІКТ сам здійснював усі перевірки, щоб переконатися, що продукти ІКТ, послуги ІКТ чи процеси ІКТ відповідають європейській системі сертифікації кібербезпеки. Самооцінку

відповідності слід вважати доцільною для продуктів ІКТ низької складності, послуг ІКТ чи ІКТ-процесів, які представляють низький ризик для населення, таких як просте проектування та виробничі механізми. Більше того, самооцінка відповідності повинна бути дозволена для продуктів ІКТ, послуг ІКТ або процесів ІКТ лише там, де вони відповідають рівню забезпечення "базовим".

Європейські схеми сертифікації кібербезпеки можуть дозволяти як самооцінку відповідності, так і сертифікацію продуктів ІКТ, послуг ІКТ чи процесів ІКТ. У такому випадку схема повинна передбачати чіткі та зрозумілі способи для споживачів чи інших користувачів розмежовувати продукти ІКТ, послуги ІКТ чи процеси ІКТ, щодо яких відповідає виробник чи постачальник продуктів ІКТ, послуг ІКТ чи процесів ІКТ. оцінку та продукти ІКТ, послуги ІКТ або процеси ІКТ, які сертифіковані третьою стороною.

Виробник або постачальник ІКТ-продуктів, послуг ІКТ чи ІКТ-процесів, які здійснюють самооцінку відповідності, повинен мати можливість видавати та підписувати декларацію про відповідність ЄС як частину процедури оцінки відповідності.

Декларація відповідності ЄС - це документ, в якому зазначається, що конкретний продукт ІКТ, послуга ІКТ або процес ІКТ відповідає вимогам європейської схеми сертифікації кібербезпеки [3]. Видаючи та підписуючи декларацію про відповідність ЄС, виробник або постачальник продуктів ІКТ, послуг ІКТ чи ІКТ-процесів бере на себе відповідальність за відповідність ІКТ-продукту, ІКТ-послуги чи ІКТ-процесу законодавчим вимогам європейської схеми сертифікації кібербезпеки.

Копію заяви про відповідність ЄС слід подати до національного органу з сертифікації кібербезпеки та до ENISA.

Виробники чи постачальники продуктів ІКТ, послуг ІКТ чи ІКТ-процесів повинні надавати заяву ЄС про відповідність, технічну документацію та всю іншу відповідну інформацію, що стосується відповідності продуктів ІКТ, послуг ІКТ чи процесів ІКТ європейській системі сертифікації кібербезпеки. компетентний національний орган із сертифікації кібербезпеки на термін, передбачений

відповідною європейською схемою сертифікації кібербезпеки. Технічна документація повинна вказувати вимоги, що застосовуються за схемою, і повинна охоплювати проектування, виготовлення та експлуатацію ІКТ-продукту, послуги ІКТ або процесу ІКТ в тій мірі, яка відповідає самооцінці відповідності.

Управління європейською системою сертифікації кібербезпеки враховує участь держав-членів, а також належне залучення зацікавлених сторін та встановлює роль Комісії під час планування та пропонування, запитування, підготовки, прийняття та перегляду європейських схем сертифікації кібербезпеки.

Комісія повинна підготувати за підтримки Європейської групи з сертифікації кібербезпеки (далі - ECCG) та Групи із сертифікації кібербезпеки зацікавлених сторін, а після відкритих і широких консультацій розгорнуту робочу програму Союзу для європейських схем сертифікації кібербезпеки та опублікувати її форма необов'язкового документа.

Постійна робоча програма Союзу повинна бути стратегічним документом, який дозволяє промисловості, національним органам влади та органам стандартизації, зокрема, заздалегідь підготуватися до майбутніх європейських схем сертифікації кібербезпеки.

Постійна робоча програма Союзу повинна включати багаторічний огляд запитів на схеми кандидатів, які Комісія має намір подати до ENISA для підготовки на основі конкретних підстав. Комісія повинна брати до уваги постійну робочу програму Союзу під час підготовки свого Плану постійної стандартизації ІКТ та запитів на стандартизацію до європейських організацій із стандартизації. У світлі швидкого впровадження та впровадження нових технологій, появи раніше невідомих ризиків кібербезпеки та законодавчого та ринкового розвитку, Комісія або ECCG повинні мати право вимагати від ENISA підготувати схеми кандидатів, які не були включені до переліку Союзу робоча програма. У таких випадках Комісія та ECCG повинні також оцінити необхідність такого запиту, беручи до уваги загальні цілі та завдання Регламенту (ЄС) 2019/881 [3] та необхідність забезпечити наступність щодо планування та використання ресурсів ENISA.

Після такого запиту ENISA повинна підготувати схеми кандидатів для конкретних продуктів ІКТ, послуг ІКТ та процесів ІКТ без зайвої затримки. Комісія повинна оцінити позитивний та негативний вплив свого запиту на конкретний ринок, про який йдеться, особливо його вплив на МСП, інновації, бар'єри для виходу на цей ринок та витрати для кінцевих споживачів. Комісія, на основі схеми кандидатів, підготовленої ENISA, повинна бути уповноважена приймати європейську схему сертифікації кібербезпеки за допомогою виконавчих актів.

Беручи до уваги загальне призначення та цілі безпеки, викладені у цьому Регламенті, європейські схеми сертифікації кібербезпеки, прийняті Комісією, повинні визначати мінімальний набір елементів, що стосуються предмету, обсягу та функціонування індивідуальної схеми. Ці елементи повинні включати, серед іншого, сферу та об'єкт сертифікації кібербезпеки, включаючи категорії продуктів ІКТ, послуги ІКТ та охоплені процеси ІКТ, детальну специфікацію вимог кібербезпеки, наприклад, посилання на стандарти або технічні специфікації, конкретні критерії оцінки та методи оцінки, а також передбачуваний рівень довіри ("базовий", "суттєвий" або "високий") та рівні оцінки, якщо це необхідно. ENISA повинна мати можливість відхилити запит ECCG. Такі рішення повинні прийматися Правлінням та повинні бути належним чином обґрунтованими, наприклад, посиланням на стандарти або технічні специфікації, конкретні критерії оцінки та методи оцінки, а також передбачуваний рівень довіри ("базовий", "суттєвий" або "високий") та рівні оцінки, де це доречно. ENISA повинна мати можливість відхилити запит ECCG. Такі рішення повинні прийматися Правлінням і повинні бути належним чином обґрунтованими. наприклад, посиланням на стандарти або технічні специфікації, конкретні критерії оцінки та методи оцінки, а також передбачуваний рівень довіри ("базовий", "суттєвий" або "високий") та рівні оцінки, де це доречно. ENISA повинна мати можливість відхилити запит ECCG. Такі рішення повинні прийматися Правлінням і повинні бути належним чином обґрунтованими.

ENISA повинна вести веб-сайт, що надає інформацію про європейські схеми

сертифікації кібербезпеки та оприлюднює їх, що включає, серед іншого, запити на підготовку схеми кандидатів, а також відгуки, отримані в процесі консультацій, проведених ENISA на етапі підготовки. Веб-сайт також повинен містити інформацію про європейські сертифікати кібербезпеки та декларації ЄС про відповідність, видані відповідно до Регламенту (ЄС) 2019/881 [3], включаючи інформацію щодо відкликання та закінчення терміну дії таких європейських сертифікатів кібербезпеки та декларацій ЄС про відповідність. На веб-сайті також слід вказати національні схеми сертифікації кібербезпеки, які були замінені європейською схемою сертифікації кібербезпеки.

1.5 Дослідження стандартизації та Європейської схеми сертифікації кібербезпеки

З моменту свого створення ENISA активно працює в галузі стандартизації, співпрацюючи з європейськими та міжнародними організаціями по розробці стандартів (ESO та SDO), такими як ETSI, CEN, CENELEC та спільноти зацікавлених сторін в галузі стандартизації NIS. Відповідно до (ЄС) No 526/2013 Європейського Парламенту та Ради [2], ENISA внесла подальший внесок в дослідження і розробку стандартів ЄС для управління ризиками та безпеки електронних продуктів, систем, мереж і послуг. Регламент (ЄС) 2019/881 встановлює європейську систему сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ і процесів ІКТ. ENISA бере участь в цій новій структурі, готуючи схеми сертифікації кандидатів на вимогу Європейської комісії або Європейської координаційної групи з кібербезпеки (представництво держав-членів).

Стандартизація відіграє важливу роль в цій структурі, оскільки згідно законодавства:

а) існує потреба в більш тісному міжнародному співробітництві для поліпшення стандартів кібербезпеки, включаючи потребу в визначеннях загальних норм поведінки, прийнятті кодексів поведінки, використанні міжнародних стандартів і обмін інформацією, сприяючи швидшому міжнародного

співробітництва у відповідь на мережеві і питання інформаційної безпеки та просування загального глобального підходу до таких питань;

б) Європейські схеми сертифікації кібербезпеки повинні бути недискримінаційними і грунтуватися на європейських або міжнародних стандартах, якщо тільки ці стандарти не є неефективними або недоречними для виконання законних цілей Союзу в цьому відношенні;

в) Сертифікат або заяву про відповідність вимогам стандартів ЄС повинні містити посилання на технічні специфікації, стандарти і процедури, пов'язані з ним;

г) Європейська схема сертифікації кібербезпеки повинна мати посилання на міжнародні, європейські та національні стандарти, що застосовуються при оцінці, або, якщо такі стандарти недоступні або не підходять, на технічні специфікації, які відповідають вимогам.

Загальна концепція ролі стандартів в процесі оцінки і сертифікації представлена на рис. 1.3 [11].

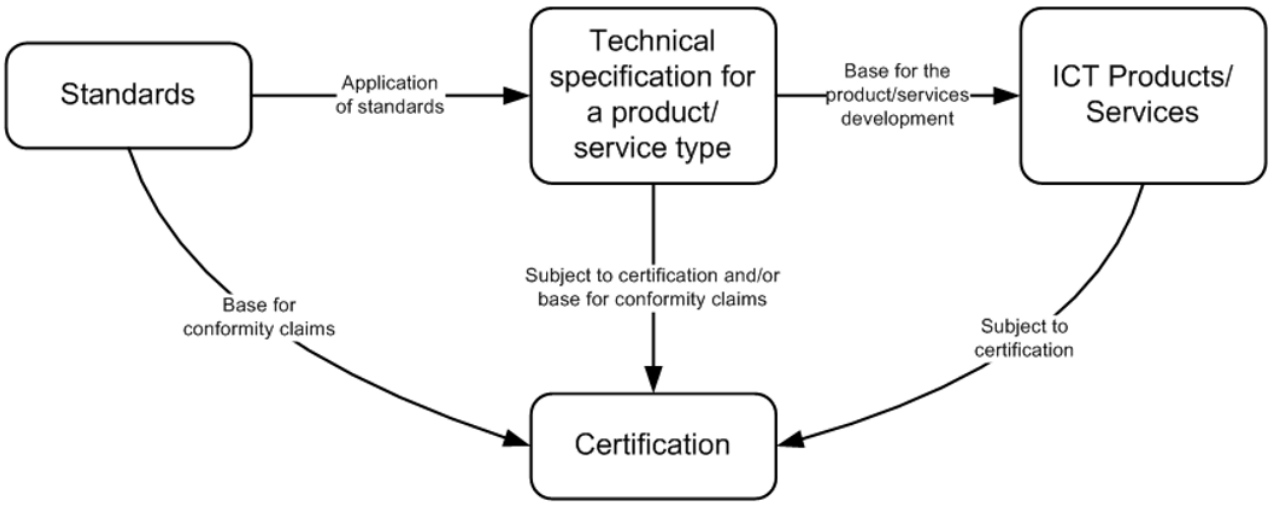

Рисунок 1.3 – Загальна концепція ролі стандартів в процесі оцінки і сертифікації

Підставою для впевненості, що продукт ІКТ, послуга ІКТ чи процес ІКТ відповідають вимогам безпеки конкретної європейської схеми сертифікації

кібербезпеки є рівень довіри європейської схеми сертифікації.

Для забезпечення узгодженості європейської системи сертифікації кібербезпеки європейська схема сертифікації кібербезпеки повинна мати можливість визначати рівні надійності європейських сертифікатів кібербезпеки та декларацій ЄС про відповідність, виданих відповідно до цієї схеми.

Кожен європейський сертифікат кібербезпеки може посилатися на один із рівнів довіри: „базовий", „суттєвий" чи „високий", тоді як декларація відповідності ЄС може стосуватися лише рівня „гарантійного".

Рівні довіри забезпечували б відповідну строгість та глибину оцінки продукту ІКТ, Служба ІКТ або процес ІКТ і характеризується посиланням на технічні специфікації, стандарти та процедури, пов'язані з ними, включаючи технічний контроль, метою якого є пом'якшення або запобігання інцидентам. Кожен рівень довіри повинен узгоджуватися між різними галузевими доменами, де застосовується сертифікація.

Європейська схема сертифікації кібербезпеки може визначати кілька рівнів оцінки залежно від суворості та глибини використаної методології оцінки. Рівні оцінки повинні відповідати одному з рівнів довіри та повинні бути пов'язані з відповідною комбінацією компонентів довіри. Для всіх рівнів довіри продукт ІКТ, послуга ІКТ чи процес ІКТ повинні містити ряд захищених функцій, як зазначено в схемі, яка може включати: безпечну конфігурацію, що підписана, підписаний код, безпечне оновлення та використовувати пом'якшення та захист повної пам'яті стека або купи. Ці функції слід було розробити та підтримувати, використовуючи підходи до розвитку, орієнтовані на безпеку, та відповідні інструменти для забезпечення надійного включення ефективних програмних та апаратних механізмів.

Щодо базового рівня довіри, оцінка повинна керуватися принаймні такими компонентами довіри: оцінка повинна щонайменше включати огляд технічної документації на ІКТ-продукт, послугу ІКТ чи процес ІКТ ООВ. Якщо сертифікація включає процеси ІКТ, процес, який використовується для проектування, розробки та обслуговування продукту ІКТ чи послуги ІКТ, також

повинен підлягати технічному огляду. Якщо європейська схема сертифікації кібербезпеки передбачає самооцінку відповідності, має бути достатнім, щоб виробник чи постачальник продуктів ІКТ, послуг ІКТ чи процесів ІКТ здійснив самооцінку відповідності продукту ІКТ, послуги ІКТ або Процес ІКТ із схемою сертифікації.

Для рівня довіри "суттєвий", крім вимог до рівня "базовий", оцінка повинна керуватися, принаймні, перевіркою відповідності функціональних можливостей продукту ІКТ, послуги ІКТ чи процесу ІКТ його технічним характеристикам документація.

Для рівня довіри "високий", окрім вимог до рівня достовірності "суттєвий", оцінка повинна керуватися принаймні тестуванням ефективності, яке оцінює стійкість функціональних можливостей продукту ІКТ, послуги ІКТ чи процесу ІКТ до складних кібератаки, що здійснюються особами, які мають значні навички та ресурси.

Звернення до європейської сертифікації кібербезпеки та до заяв ЄС про відповідність повинно залишатися добровільним, якщо інше не передбачено законодавством Союзу або законодавством держав-членів, прийнятим відповідно до законодавства Союзу. За відсутності гармонізованого законодавства Союзу держави-члени можуть прийняти національні технічні регламенти, що передбачають обов'язкову сертифікацію за європейською схемою сертифікації кібербезпеки відповідно до Директиви (ЄС) 2015/1535 Європейського Парламенту та Ради. Держави-члени також звертаються до європейської сертифікації кібербезпеки в контексті державних закупівель та Директиви 2014/24/ЄС Європейського Парламенту та Ради.

У деяких сферах може знадобитися в майбутньому встановити конкретні вимоги щодо кібербезпеки та зробити їх сертифікацію обов'язковою для певних продуктів ІКТ, послуг ІКТ або процесів ІКТ, щоб поліпшити рівень кібербезпеки в Союзі. Комісія повинна регулярно контролювати вплив прийнятих європейських схем сертифікації кібербезпеки на доступність безпечних продуктів ІКТ, послуг ІКТ та процесів ІКТ на внутрішньому ринку та повинна регулярно

оцінювати рівень використання схем сертифікації виробниками або постачальниками продуктів ІКТ. Послуги ІКТ або процеси ІКТ в Союзі. Ефективність європейських схем сертифікації кібербезпеки, а також те, чи слід робити певні схеми обов'язковими, слід оцінювати з урахуванням законодавства Союзу, пов'язаного з кібербезпекою, зокрема Директиви (ЄС) 2016/1148 [4], беручи до уваги безпеку мережеві та інформаційні системи, що використовуються операторами основних послуг.

Європейські сертифікати кібербезпеки та декларації відповідності ЄС повинні допомогти кінцевим споживачам робити обґрунтований вибір. Тому продукти ІКТ, послуги ІКТ та процеси ІКТ, які були сертифіковані або для яких видано декларацію про відповідність ЄС, повинні супроводжуватися структурованою інформацією, яка адаптована до очікуваного технічного рівня запланованого кінцевого споживача. Вся така інформація повинна бути доступна в Інтернеті та, у відповідних випадках, у фізичній формі. Кінцевий користувач повинен мати доступ до інформації щодо контрольного номера схеми сертифікації, рівня довіри, опису ризиків кібербезпеки, пов’язаних із продуктом ІКТ, послугою ІКТ чи процесом ІКТ, та органом, що видає інформацію, або повинен мати можливість отримати копію європейського сертифіката кібербезпеки. В додаток, кінцевий користувач повинен бути проінформований про політику підтримки кібербезпеки, а саме про те, як довго кінцевий користувач може розраховувати на отримання оновлень або виправлень кібербезпеки, про виробника чи постачальника продуктів ІКТ, послуг ІКТ чи процесів ІКТ. Там, де це застосовно, вказівки щодо дій або налаштувань, які кінцевий користувач може застосувати для підтримання або підвищення кібербезпеки продукту ІКТ або послуги ІКТ, а також контактна інформація єдиного контактного пункту для звітування та отримання підтримки у випадку кібератак (у на додаток до автоматичної звітності). Цю інформацію слід регулярно оновлювати та розміщувати на веб-сайті, що містить інформацію про європейські схеми сертифікації кібербезпеки. виробника або постачальника ІКТ-продуктів, ІКТ-послуг чи ІКТ-процесів. Там, де це застосовно, вказівки щодо дій або

налаштувань, які кінцевий користувач може застосувати для підтримання або підвищення кібербезпеки продукту ІКТ або послуги ІКТ, а також контактна інформація єдиного контактного пункту для звітування та отримання підтримки у випадку кібератак (у на додаток до автоматичної звітності). Цю інформацію слід регулярно оновлювати та розміщувати на веб-сайті, що містить інформацію про європейські схеми сертифікації кібербезпеки. виробника або постачальника продуктів ІКТ, послуг ІКТ або процесів ІКТ. Там, де це застосовно, вказівки щодо дій або налаштувань, які кінцевий користувач може застосувати для підтримання або підвищення кібербезпеки продукту ІКТ або послуги ІКТ, а також контактна інформація єдиного контактного пункту для звітування та отримання підтримки у випадку кібератак (у на додаток до автоматичної звітності). Цю інформацію слід регулярно оновлювати та розміщувати на веб-сайті, що містить інформацію про європейські схеми сертифікації кібербезпеки. вказівки щодо дій або налаштувань, які кінцевий користувач може застосувати для підтримання або підвищення кібербезпеки продукту ІКТ або послуги ІКТ, а також контактна інформація єдиного контактного пункту для звітування та отримання підтримки у разі кібератак (крім автоматичних звітність). Цю інформацію слід регулярно оновлювати та розміщувати на веб-сайті, що містить інформацію про європейські схеми сертифікації кібербезпеки. вказівки щодо дій чи налаштувань, які кінцевий користувач може застосувати для підтримання або підвищення кібербезпеки продукту ІКТ або послуги ІКТ, а також контактна інформація єдиного контактного пункту для повідомлення та отримання підтримки у разі кібератак (на додаток до автоматичних звітність). Цю інформацію слід регулярно оновлювати та розміщувати на веб-сайті, що містить інформацію про європейські схеми сертифікації кібербезпеки.

З метою досягнення цілей Регламенту (ЄС) 2019/881 [3] та уникнення фрагментації внутрішнього ринку національні схеми або процедури сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ чи ІКТ, що охоплюються європейською схемою сертифікації кібербезпеки, повинні перестати діяти з дати, встановленої Комісією за допомогою виконавчих актів.

Більше того, держави-члени не повинні запроваджувати нові національні схеми сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ чи процесів ІКТ, які вже охоплені існуючою європейською системою сертифікації кібербезпеки. Однак державам-членам не слід заважати приймати або підтримувати національні схеми сертифікації кібербезпеки для цілей національної безпеки. Держави-члени повинні інформувати Комісію та ECCG про будь-який намір скласти нові національні схеми сертифікації кібербезпеки. Комісія та ECCG повинні оцінити вплив нових національних схем сертифікації кібербезпеки на належне функціонування внутрішнього ринку та у світлі будь-якого стратегічного інтересу щодо подання запиту щодо європейської схеми сертифікації кібербезпеки.

Європейські схеми сертифікації кібербезпеки мають на меті допомогти гармонізувати практики кібербезпеки в межах Союзу. Вони повинні сприяти підвищенню рівня кібербезпеки в межах Союзу. Дизайн європейських схем сертифікації кібербезпеки повинен враховувати та дозволяти розробляти інновації у галузі кібербезпеки.

Європейські схеми сертифікації кібербезпеки повинні враховувати сучасні методи розробки програмного та апаратного забезпечення та, зокрема, вплив частого оновлення програмного забезпечення чи мікропрограми на окремі європейські сертифікати кібербезпеки. Європейські схеми сертифікації кібербезпеки повинні визначати умови, за яких оновлення може вимагати повторної сертифікації продукту ІКТ, послуги ІКТ або процесу ІКТ або зменшення обсягу конкретного європейського сертифіката кібербезпеки з урахуванням будь-яких можливих негативних наслідків оновлення на відповідність вимогам безпеки цього сертифіката.

Після того, як буде прийнята європейська схема сертифікації кібербезпеки, виробники або постачальники продуктів ІКТ, послуг ІКТ або процесів ІКТ повинні мати можливість подавати заявки на сертифікацію своїх продуктів ІКТ чи послуг ІКТ до ООВ на їх вибір у будь-якій точці Союзу. ООВ повинні бути акредитовані національним органом з акредитації, якщо вони відповідають певним зазначеним вимогам, встановленим у цьому Регламенті. Акредитація

повинна видаватися максимум на п’ять років і повинна поновлюватися на тих самих умовах за умови, що ООВ все ще відповідає вимогам. Національні органи з акредитації повинні обмежити, призупинити або анулювати акредитацію ООВ, якщо умови акредитації не були дотримані або вже не виконуються, або коли ООВ порушує Регламент (ЄС) 2019/881 [3].

Посилання у національному законодавстві на національні стандарти, які перестали діяти через набрання чинності європейською схемою сертифікації кібербезпеки, можуть викликати плутанину. Отже, держави-члени повинні відображати прийняття європейської схеми сертифікації кібербезпеки у своєму національному законодавстві.

Для досягнення еквівалентних стандартів у всьому Союзі, сприяння взаємному визнанню та сприяння загальному прийняттю європейських сертифікатів кібербезпеки та декларацій про відповідність ЄС, необхідно запровадити систему експертного оцінювання між національними органами з сертифікації кібербезпеки.

Експертна перевірка повинна охоплювати процедури нагляду за відповідністю продуктів ІКТ, послуг ІКТ та процесів ІКТ європейським сертифікатам кібербезпеки, контролю за зобов'язаннями виробників або постачальників продуктів ІКТ, послуг ІКТ чи ІКТ, які здійснюють самооцінку відповідності, для моніторинг ООВ, а також доцільність експертизи персоналу органів, що видають сертифікати на рівень довіри „високий”. Комісія повинна мати можливість шляхом імплементаційних актів скласти принаймні п'ятирічний план експертних оцінок, а також встановити критерії та методології функціонування системи експертної оцінки.

Без шкоди загальній системі експертної перевірки, яка буде запроваджена в усіх національних органах з сертифікації кібербезпеки в рамках європейської системи сертифікації кібербезпеки, певні європейські схеми сертифікації кібербезпеки можуть включати механізм оцінки експертних оцінок для органів, які видають європейські сертифікати кібербезпеки для продуктів ІКТ, Послуги ІКТ та процеси ІКТ із рівнем довіри за такими схемами є "високим".

ECCG повинна підтримувати впровадження таких механізмів експертної оцінки. Партнерські оцінки повинні, зокрема, оцінювати, чи виконують відповідні органи свої завдання узгоджено, і можуть включати механізми оскарження. Результати експертних оцінок повинні бути загальнодоступними. Зацікавлені органи можуть прийняти відповідні заходи, щоб відповідно адаптувати свою практику та досвід.

1.6 Аналіз порядку призначення державами-членами ЄС національних органів з сертифікації кібербезпеки згідно Регламенту (ЄС) 2019/881

Держави-члени повинні призначити один або кілька національних органів з сертифікації кібербезпеки для нагляду за дотриманням зобов'язань, що випливають із Регламенту (ЄС) 2019/881 [3].

Національним органом з сертифікації кібербезпеки може бути існуючий або новий орган. Держава-член також повинна мати можливість призначити, після узгодження з іншою державою-членом, одного або декількох національних органів з сертифікації кібербезпеки на території цієї іншої держави-члена.

Національні органи з сертифікації кібербезпеки повинні також розглядати скарги, подані фізичними або юридичними особами стосовно європейських сертифікатів кібербезпеки, виданих цими органами влади, або стосовно європейських сертифікатів кібербезпеки, виданих ООВ, якщо такі сертифікати свідчать про рівень довіри «високий», слід провести розслідування, наскільки це можливо, предмет скарги і повинен інформувати скаржника про хід та результати розслідування протягом розумного періоду. Більше того, національні органи з сертифікації кібербезпеки повинні співпрацювати з іншими національними органами з сертифікації кібербезпеки або іншими державними органами, в тому числі шляхом обміну інформацією про можливу невідповідність продуктів ІКТ, Послуги ІКТ та процеси ІКТ з вимогами Регламенту (ЄС) 2019/881 [3] або з конкретними європейськими схемами сертифікації кібербезпеки. Комісія повинна сприяти такому обміну інформацією, надаючи загальну електронну систему

інформаційної підтримки, наприклад, Інформаційно-комунікаційну систему з нагляду за ринком (ICSMS) та систему швидкого оповіщення про небезпечні непродовольчі товари (RAPEX), яка вже використовується ринком органи нагляду відповідно до Регламенту (ЄС) No 765/2008 [7].

З метою забезпечення послідовного застосування європейської системи сертифікації кібербезпеки слід створити ECCG, що складається з представників національних органів з сертифікації кібербезпеки або інших відповідних національних органів. Член ECCG не повинен представляти більше двох держав-членів.

Зацікавлені сторони та відповідні треті сторони можуть бути запрошені брати участь у засіданнях ECCG та брати участь у її роботі.

ECCG повинна мати такі завдання [3]:

а) консультувати та допомагати Комісії в її роботі щодо забезпечення послідовного впровадження та застосування постійної робочої програми Союзу, питань політики сертифікації кібербезпеки, координації політичних підходів та підготовки європейських схем сертифікації кібербезпеки;

б) допомагати, консультувати та співпрацювати з ENISA щодо підготовки схеми кандидатів відповідно до статті 49 Регламенту (ЄС) 2019/881;

в) прийняти висновок щодо схем кандидатів, підготовлених ENISA відповідно до статті 49 Регламенту (ЄС) 2019/881;

г) просити ENISA підготувати схеми кандидатів відповідно до статті 48 (2) Регламенту (ЄС) 2019/881;

д) прийняти висновки, адресовані Комісії, щодо обслуговування та перегляду існуючих європейських схем сертифікації кібербезпеки;

е) вивчити відповідні події у галузі сертифікації кібербезпеки та обмінятися інформацією та передовою практикою щодо схем сертифікації кібербезпеки;

ж) сприяти співпраці між національними органами з сертифікації кібербезпеки шляхом створення потенціалу та обміну інформацією, зокрема шляхом встановлення методів ефективного обміну інформацією, що стосується

питань, що стосуються сертифікації кібербезпеки;

з) підтримати впровадження механізмів експертної оцінки згідно з правилами, встановленими в європейській схемі сертифікації кібербезпеки відповідно до пункту (u) статті 54 (1) Регламенту (ЄС) 2019/881;

и) сприяти узгодженню європейських схем сертифікації кібербезпеки з міжнародно визнаними стандартами, в тому числі шляхом перегляду існуючих європейських схем сертифікації кібербезпеки та, де це доцільно, надання рекомендацій ENISA щодо взаємодії з відповідними міжнародними організаціями стандартизації для усунення недоліків або прогалин у міжнародно визнаних стандартах.

За сприяння ENISA Комісія головує в ECCG, а Комісія надає ECCG секретаріат.

З метою підвищення обізнаності та сприяння прийняттю майбутніх європейських схем сертифікації кібербезпеки, Комісія може видати загальні або галузеві керівні принципи кібербезпеки, наприклад щодо належної практики кібербезпеки або відповідальної поведінки кібербезпеки, підкреслюючи позитивний ефект від використання сертифікованих продуктів ІКТ. Послуги ІКТ та процеси ІКТ.

З метою подальшого сприяння торгівлі та визнання того, що ланцюжки постачання ІКТ є глобальними, Союз може укласти угоди про взаємне визнання щодо європейських сертифікатів кібербезпеки відповідно до статті 218 Договору про функціонування Європейського Союзу (ДФЕС). Комісія, беручи до уваги поради ENISA та Європейської групи з сертифікації кібербезпеки, може рекомендувати розпочати відповідні переговори. Кожна європейська схема сертифікації кібербезпеки повинна передбачати конкретні умови для таких угод про взаємне визнання з третіми країнами.

З метою забезпечення єдиних умов для імплементації Регламенту (ЄС) 2019/881 [3], виконавчі повноваження повинні бути наділені Комісією. Ці повноваження слід здійснювати відповідно до Регламенту (ЄС) № 182/2011 Європейського Парламенту та Ради.

Процедуру експертизи слід застосовувати для прийняття актів, що реалізують європейські схеми сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ або процесів ІКТ, для прийняття актів, що стосуються механізмів проведення запитів з боку ENISA, для прийняття актів про імплементацію. план для експертної перевірки національних органів з сертифікації кібербезпеки, а також для прийняття імплементаційних актів щодо обставин, форматів та процедур повідомлень акредитованих ООВ національними органами з сертифікації кібербезпеки Комісії.

Діяльність ENISA повинна проходити регулярну та незалежну оцінку. Ця оцінка повинна враховувати цілі ENISA, її робочу практику та відповідність її завдань, зокрема його завдань, що стосуються оперативного співробітництва на рівні Союзу. Ця оцінка повинна також оцінити вплив, результативність та ефективність європейської системи сертифікації кібербезпеки. У разі перегляду Комісія повинна оцінити, як можна посилити роль ENISA як орієнтира для консультацій та досвіду, а також оцінити можливість ролі ENISA у підтримці оцінки продуктів ІКТ, послуг ІКТ та ІКТ третіх країн. процеси, які не відповідають правилам Союзу, коли такі товари, послуги та процеси потрапляють до Союзу.

Оскільки цілі Регламенту (ЄС) 2019/881 не можуть бути в достатній мірі досягнуті державами-членами, але, швидше за все, через його масштаби та наслідки можуть бути краще досягнуті на рівні Союзу, Союз може приймати заходи відповідно до принципу субсидіарності, як встановлено в Стаття 5 Договору про Європейський Союз. Відповідно до принципу пропорційності, викладеного в цій статті, цей Регламент не виходить за рамки того, що необхідно для досягнення цих цілей та скасовує Регламент (ЄС) No 526/2013 [2].

1.7 Висновки з розділу 1

Розділ присвячений дослідженню шляхів забезпечення кібербезпеки та підвищення рівня довіри до цифрових технологій в Європейському Союзі, які

запроваджуються зараз та будуть мати вплив на аналогічні процеси в Україні.

Показано, що мережеві й інформаційні системи та електронні комунікаційні мережі й послуги в ЄС розглядаються як основа економічного зростання. Разом з тим ЄС такий стан речей розглядає і як джерело потужних кіберзагроз в майбутньому.

Аналіз шляхів забезпечення кібербезпеки та підвищення довіри до цифрових технологій в ЄС спонукав до створення Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та прийняття на загальносоюзному просторі у 2019 році Акту про кібербезпеку (Регламент ЄС 2019/881).

Одним з базових механізмів підвищенні довіри та безпеки до інформаційних та телекомунікаційних технологій у Акті про кібербезпеку визначено створення Європейської системи сертифікації кібербезпеки, в тому числі Європейської схеми сертифікації кібербезпеки та порядку призначення державами-членами ЄС національних органів з сертифікації кібербезпеки.

2 ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ ШЛЯХОМ ДОСЛІДЖЕННЯ ТА РОЗВ'ЯЗАННЯ ПРОБЛЕМ СЕРТИФІКАЦІЇ ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ЩОДО КІБЕРБЕЗПЕКИ НА ВІДПОВІДНІСТЬ ВИМОГАМ АКТУ З КІБЕРБЕЗПЕКИ ЄС

2.1 Мета створення гармонізованої з європейською національної системи сертифікації кібербезпеки

Національна система сертифікації кібербезпеки повинна бути створена з метою поліпшення умов для функціонування внутрішнього ринку шляхом підвищення рівня кібербезпеки в межах України та забезпечення гармонізованого підходу на рівні України до європейських схем сертифікації кібербезпеки з метою створення єдиного цифрового ринку для ІКТ-продуктів, ІКТ-послуг та ІКТ-процесів.

Національна система сертифікації кібербезпеки повинна передбачати механізм встановлення європейських схем сертифікації кібербезпеки та підтвердження того, що продукти ІКТ, послуги ІКТ та процеси ІКТ, які були оцінені відповідно до таких схем, відповідають визначеним вимогам безпеки з метою захисту доступність, достовірність, цілісність або конфіденційність збережених або переданих або оброблених даних або функцій або послуг, що пропонуються або доступні через ці продукти, послуги та процеси протягом їх життєвого циклу.

Для європейської сертифікації кібербезпеки створена постійна робоча програма Союзу, яка, зокрема, включає перелік продуктів ІКТ, послуг ІКТ та процесів ІКТ або їх категорії, які можуть отримати користь від включення до сфери європейської схеми сертифікації кібербезпеки [3].

Включення конкретних продуктів ІКТ, послуг ІКТ та процесів ІКТ або їх категорій до постійної робочої програми Союзу повинно бути виправданим на підставі однієї або декількох з таких підстав:

а) наявність та розробка національних схем сертифікації кібербезпеки, що

охоплюють певну категорію продуктів ІКТ, послуг ІКТ чи процесів ІКТ, і зокрема, щодо ризику фрагментації;

б) відповідний закон чи політика Союзу чи держави-члена;

в) ринковий попит;

г) розвиток ландшафту кіберзагроз;

д) запит на підготовку конкретної схеми кандидатів з боку ECCG.

Європейська комісія належним чином враховує думки, випущені ECCG та групою з сертифікації зацікавлених сторін щодо проекту постійної робочої програми Союзу.

Перша робоча програма Союзу опублікована до 28 червня 2020 року. Програма постійної роботи Союзу оновлюється принаймні раз на три роки і частіше за необхідності.

Запит на європейську схему сертифікації кібербезпеки наступний.

Комісія може вимагати від ENISA підготувати схему кандидатів або переглянути існуючу європейську схему сертифікації кібербезпеки на основі постійної робочої програми Союзу.

У належним чином обґрунтованих випадках Комісія або ECCG можуть вимагати від ENISA підготувати схему кандидатів або переглянути існуючу європейську схему сертифікації кібербезпеки, яка не включена до постійної робочої програми Союзу. Постійна програма роботи Союзу повинна бути відповідно оновлена.

Підготовка, прийняття та перегляд європейської схеми сертифікації кібербезпеки здійнюється згідно ст. 49 Регламенту (ЄС) 2019/881 Європейського Парламенту та Ради [3].

Національна система сертифікації кібербезпеки як і європейська повинна вести спеціальний веб-сайт, що надає інформацію про національні схеми сертифікації кібербезпеки, національні сертифікати кібербезпеки та декларації про відповідність, включаючи інформацію стосовно національних схем сертифікації кібербезпеки, які вже не діють, та про вилучену національну кібербезпеку та термін дії якої закінчився, сертифікати та декларації про

відповідність, а також на сховище посилань на інформацію про кібербезпеку.

Там, де це можливо, на веб-сайті також зазначаються національні схеми сертифікації кібербезпеки, які були замінені європейською схемою сертифікації кібербезпеки.

2.2 Цілі безпеки та рівні довіри в європейських та національних схемах сертифікації кібербезпеки

Національна схема сертифікації кібербезпеки як і європейська схема повинна бути розроблена для досягнення, залежно від ситуації, щонайменше наступних цілей безпеки:

а) для захисту даних, що зберігаються, передаються або обробляються іншим чином від випадкового або несанкціонованого зберігання, обробки, доступу або розкриття інформації протягом усього життєвого циклу ІКТ-продукту, послуги ІКТ або процесу ІКТ;

б) для захисту даних, що зберігаються, передаються або обробляються іншим чином від випадкового або несанкціонованого знищення, втрати чи зміни або відсутності доступності протягом усього життєвого циклу ІКТ-продукту, послуги ІКТ або процесу ІКТ;

в) що уповноважені особи, програми або машини можуть мати доступ лише до даних, послуг або функцій, на які посилаються їх права доступу;

г) виявити та документувати відомі залежності та вразливості;

д) реєструвати, до яких даних, послуг чи функцій, в який час та ким здійснювався доступ, використання чи інша обробка;

е) щоб можна було перевірити, до яких даних, послуг чи функцій здійснювався доступ, використання чи обробка в інший спосіб, в який час та ким;

ж) перевірити, що продукти ІКТ, послуги ІКТ та процеси ІКТ не містять відомих вразливостей;

з) своєчасно відновлювати доступність та доступ до даних, послуг та функцій у разі фізичного чи технічного інциденту;

и) що продукти ІКТ, послуги ІКТ та процеси ІКТ захищені за замовчуванням та за проектом;

к) що продукти ІКТ, послуги ІКТ та процеси ІКТ забезпечуються сучасним програмним та апаратним забезпеченням, яке не містить загальновідомих вразливих місць, а також механізмами безпечного оновлення.

Європейська схема сертифікації кібербезпеки може визначати один або декілька з наступних рівнів довіри продуктів ІКТ, послуг ІКТ та процесів ІКТ: „базовий", „суттєвий" чи „високий" (рис. 2.1).

Рівень довіри повинен відповідати рівню ризику, пов'язаного із передбачуваним використанням продукту ІКТ, послуги ІКТ або процесу ІКТ, з точки зору ймовірності та впливу інциденту.

Європейські сертифікати кібербезпеки та декларації ЄС про відповідність мають стосуватися будь-якого рівня впевненості, зазначеного в європейській схемі сертифікації кібербезпеки, згідно з яким видається європейський сертифікат кібербезпеки або декларація ЄС про відповідність.

Вимоги до безпеки, що відповідають кожному рівню забезпечення, повинні бути передбачені відповідною європейською схемою сертифікації кібербезпеки, включаючи відповідні функціональні можливості безпеки та відповідну строгість та глибину оцінки, яку повинен пройти продукт ІКТ, послуга ІКТ чи процес ІКТ.

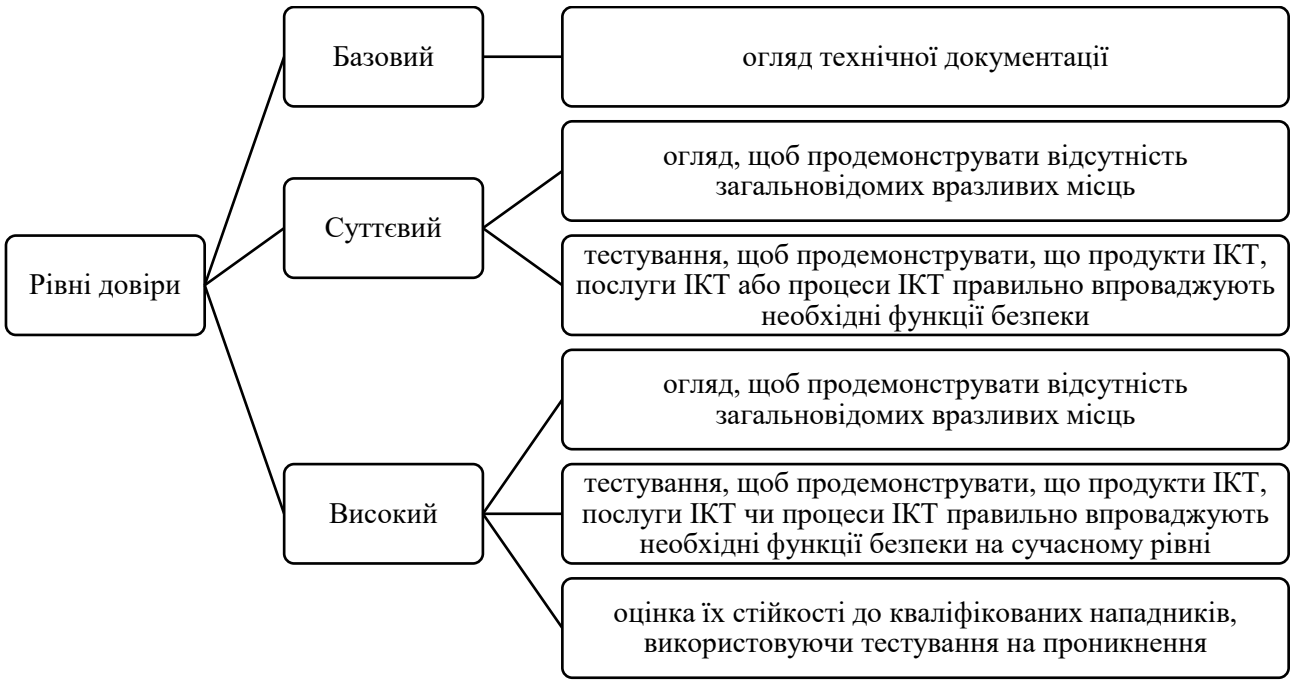

Рисунок 2.1 - Рівні довіри продуктів ІКТ, послуг ІКТ та процесів ІКТ

Сертифікат або декларація про відповідність ЄС повинні посилатися на технічні специфікації, стандарти та процедури, пов’язані з ними, включаючи технічний контроль, метою якого є зменшення ризику або запобігання інцидентам кібербезпеки.

Європейський сертифікат кібербезпеки або заява ЄС про відповідність, що стосується рівня довіри „базовий”, повинен гарантувати, що продукція ІКТ, послуги ІКТ та процеси ІКТ, для яких видається цей сертифікат або заява ЄС про відповідність, відповідають відповідним вимогам безпеки, включаючи функціональні можливості безпеки, і що вони були оцінені на рівні, призначеному для мінімізації відомих основних ризиків інцидентів та кібератак. Заходи з оцінки, які слід провести, повинні включати принаймні огляд технічної документації. Якщо такий огляд не є доцільним, слід проводити замінні заходи з оцінки з рівноцінним ефектом.

Європейський сертифікат кібербезпеки, який посилається на рівень довіри "суттєвий", повинен гарантувати, що продукти ІКТ, послуги ІКТ та процеси ІКТ, для яких видається цей сертифікат, відповідають відповідним вимогам безпеки, включаючи функціональні можливості безпеки, і що вони були оцінені на рівень,

призначений мінімізувати відомі ризики кібербезпеки, а також ризик інцидентів та кібератак, що здійснюються суб'єктами, що мають обмежені навички та ресурси. Заходи з оцінки, які слід здійснити, повинні включати щонайменше наступне:

а) огляд, щоб продемонструвати відсутність загальновідомих вразливих місць;

б) тестування, щоб продемонструвати, що продукти ІКТ, послуги ІКТ або процеси ІКТ правильно впроваджують необхідні функції безпеки.

Якщо такі заходи з оцінки не є доречними, повинні проводитись замінні дії з оцінкою з еквівалентним ефектом.

Європейський сертифікат кібербезпеки, який посилається на рівень довіри „високий", повинен гарантувати, що продукти ІКТ, послуги ІКТ та процеси ІКТ, для яких видано цей сертифікат, відповідають відповідним вимогам безпеки, включаючи функціональні можливості безпеки, і що вони були оцінені на рівень, призначений для мінімізації ризику сучасних кібератак, що здійснюються акторами, що володіють значними навичками та ресурсами. Заходи з оцінки, які слід провести, повинні включати щонайменше наступне:

а) огляд, щоб продемонструвати відсутність загальновідомих вразливих місць;

б) тестування, щоб продемонструвати, що продукти ІКТ, послуги ІКТ чи процеси ІКТ правильно впроваджують необхідні функції безпеки на сучасному рівні;

в) оцінка їх стійкості до кваліфікованих нападників, використовуючи тестування на проникнення.

Європейська схема сертифікації кібербезпеки може визначати кілька рівнів оцінки залежно від суворості та глибини використаної методології оцінки. Кожен з рівнів оцінки повинен відповідати одному з рівнів довіри та визначатися відповідною комбінацією компонентів довіри.

Європейська схема сертифікації кібербезпеки може допускати самооцінку відповідності на виключну відповідальність виробника або постачальника

продуктів ІКТ, послуг ІКТ чи процесів ІКТ. Самооцінка відповідності допускається лише стосовно продуктів ІКТ, послуг ІКТ та процесів ІКТ, які представляють низький ризик, що відповідає рівню довіри "базовий".

Виробник або постачальник продуктів ІКТ, послуг ІКТ або процесів ІКТ може видати заяву ЄС про відповідність, в якій зазначається, що продемонстровано виконання вимог, викладених у схемі. Видаючи таку заяву, виробник або постачальник продуктів ІКТ, послуг ІКТ або процесів ІКТ бере на себе відповідальність за відповідність продукту ІКТ, послуги ІКТ або процесу ІКТ вимогам, викладеним у цій схемі.

Виробник або постачальник продуктів ІКТ, послуг ІКТ чи процесів ІКТ повинен подати заяву ЄС про відповідність, технічну документацію та всю іншу відповідну інформацію, що стосується відповідності продуктів ІКТ чи послуг ІКТ схемі, доступній національній кібербезпеці сертифікаційний орган протягом періоду, передбаченого відповідною європейською схемою сертифікації кібербезпеки. Копія заяви про відповідність ЄС подається до національного органу з сертифікації кібербезпеки та до ENISA.

Видання декларації про відповідність ЄС є добровільним, якщо інше не встановлено законодавством Союзу або законодавством держав-членів.

Заяви про відповідність ЄС повинні визнаватися у всіх державах-членах.

2.3 Дослідження елементів європейських схем сертифікації кібербезпеки

Європейська схема сертифікації кібербезпеки повинна включати принаймні такі елементи:

а) предмет та обсяг схеми сертифікації, включаючи тип або категорії продуктів ІКТ, послуги ІКТ та охоплені процеси ІКТ;

б) чіткий опис мети схеми та того, як обрані стандарти, методи оцінки та рівні довіри відповідають потребам передбачуваних користувачів схеми;

в) посилання на міжнародні, європейські або національні стандарти, що застосовуються при оцінці, або, якщо такі стандарти відсутні або доречні, на

технічні специфікації, які відповідають вимогам, встановленим у Додатку II до Регламенту (ЄС) No 1025/2012 [8], або, якщо такі специфікації не доступні до технічних специфікацій чи інших вимог щодо кібербезпеки, визначених у європейській схемі сертифікації кібербезпеки;

г) де це можливо, один або більше рівнів довіри;

д) вказівка на те, чи дозволена самооцінка відповідності за схемою;

е) де це можливо, конкретні або додаткові вимоги, до яких підлягають ООВ, щоб гарантувати їх технічну компетентність для оцінки вимог щодо кібербезпеки;

ж) конкретні критерії та методи оцінки, які слід використовувати, включаючи види оцінки, для демонстрації досягнення цілей безпеки, зазначених у п.2.2 цієї магістерської роботи;

з) де це доречно, інформація, яка необхідна для сертифікації і яка повинна бути надана або іншим чином надана ООВ заявником;

и) де схема передбачає знаки або ярлики, умови, за яких такі знаки або етикетки можуть використовуватися;

к) правила моніторингу відповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам європейських сертифікатів кібербезпеки або заяв ЄС про відповідність, включаючи механізми, що демонструють постійну відповідність зазначеним вимогам кібербезпеки;

л) де це можливо, умови видачі, підтримання, продовження та поновлення європейських сертифікатів кібербезпеки, а також умови розширення або зменшення сфери сертифікації;

м) правила щодо наслідків для продуктів ІКТ, послуг ІКТ та процесів ІКТ, які були сертифіковані або для яких видано декларацію відповідності ЄС, але які не відповідають вимогам схеми;

н) правила щодо того, як повідомляти та розглядати раніше не виявлені вразливості кібербезпеки в продуктах ІКТ, послугах ІКТ та процесах ІКТ;

о) де це можливо, правила щодо зберігання записів ООВ;

п) визначення національних або міжнародних схем сертифікації

кібербезпеки, що охоплюють один і той самий тип або категорії продуктів ІКТ, послуг ІКТ та процесів ІКТ, вимог безпеки, критеріїв та методів оцінки та рівнів забезпечення;

р) зміст та формат європейських сертифікатів кібербезпеки та декларацій про відповідність ЄС, які будуть видані;

с) період доступності декларації про відповідність ЄС, технічної документації та всієї іншої відповідної інформації, яка повинна бути доступною виробнику чи постачальнику ІКТ-продуктів, послуг ІКТ чи ІКТ-процесів;

т) максимальний термін дії європейських сертифікатів кібербезпеки, виданих за схемою;

у) політика розкриття інформації про європейські сертифікати кібербезпеки, видані, змінені або скасовані за схемою;

ф) умови взаємного визнання схем сертифікації з третіми країнами;

х) де це застосовно, правила щодо будь-якого механізму експертної оцінки, встановленого схемою для органів чи органів, що видають європейські сертифікати кібербезпеки для рівня довіри "високий". Такий механізм не повинен перешкоджати експертній оцінці, передбаченій у п.2.6 цієї магістерської роботи;

ц) формату та процедур, яких повинні дотримуватися виробники чи постачальники продуктів ІКТ, послуг ІКТ чи ІКТ-процесів при наданні та оновленні додаткової інформації про кібербезпеку.

Додаткова інформація про кібербезпеку для сертифікованих продуктів ІКТ, послуг ІКТ та процесів ІКТ передбачає наступне.

Виробник або постачальник сертифікованих ІКТ-продуктів, ІКТ-послуг чи ІКТ-процесів або ІКТ-продуктів, ІКТ-послуг та ІКТ-процесів, щодо яких видано декларацію про відповідність ЄС, повинен зробити загальнодоступним наступну додаткову інформацію про кібербезпеку:

а) вказівки та рекомендації щодо допомоги кінцевим користувачам у безпечній конфігурації, встановленні, розгортанні, експлуатації та обслуговуванні продуктів ІКТ чи послуг ІКТ;

б) період, протягом якого кінцевим споживачам буде пропонуватися

підтримка безпеки, зокрема щодо доступності оновлень, пов’язаних з кібербезпекою;

в) контактна інформація виробника або постачальника та прийняті методи отримання інформації про вразливість від кінцевих користувачів та дослідників безпеки;

г) посилання на Інтернет-сховища з переліком публічно розкритих вразливих місць, пов’язаних із продуктом ІКТ, послугою ІКТ чи процесом ІКТ, а також на будь-які відповідні рекомендації щодо кібербезпеки.

Ця інформація повинна бути доступною в електронній формі, залишатиметься доступною та оновлюватися за необхідності принаймні до закінчення терміну дії відповідного європейського сертифікату кібербезпеки або декларації ЄС про відповідність.

Визначені вимоги європейської схеми сертифікації кібербезпеки повинні узгоджуватися з усіма застосовними правовими вимогами, зокрема вимогами, що випливають із гармонізованого законодавства Союзу.

Якщо конкретний правовий акт Союзу це передбачає, сертифікат або заява ЄС про відповідність, видані відповідно до європейської схеми сертифікації кібербезпеки, можуть бути використані для демонстрації презумпції відповідності вимогам цього правового акту.

За відсутності гармонізованого законодавства Союзу законодавство України може також передбачати, що європейська схема сертифікації кібербезпеки може використовуватися для встановлення презумпції відповідності законодавчим вимогам.

2.4 Сертифікація кібербезпеки в Україні та національні схеми й сертифікати

Продукти ІКТ, послуги ІКТ та процеси ІКТ, які були сертифіковані відповідно до європейської схеми сертифікації кібербезпеки, вважаються такими, що відповідають вимогам такої схеми.

Сертифікація кібербезпеки є добровільною, якщо інше не встановлено

законодавством Союзу або законодавством України.

Комісія регулярно проводить оцінку ефективності та використання прийнятих європейських схем сертифікації кібербезпеки, а також те, чи слід зробити певну європейську схему сертифікації кібербезпеки обов'язковою відповідно до законодавства Союзу, щоб забезпечити належний рівень кібербезпеки продуктів ІКТ, послуг ІКТ та ІКТ процесів у Союзі та покращити функціонування внутрішнього ринку. Перша така оцінка проводиться до 31 грудня 2023 року, а наступні оцінки проводяться принаймні кожні два роки після цього. На основі результатів цих оцінок Комісія визначає продукти ІКТ, послуги ІКТ та процеси ІКТ, що охоплюються існуючою схемою сертифікації, яка повинна охоплюватися обов'язковою схемою сертифікації.

Як пріоритет, Комісія зосередиться на секторах, перелічених у Додатку II до Директиви (ЄС) 2016/1148 [4], які оцінюватимуться не пізніше двох років після прийняття першої європейської схеми сертифікації кібербезпеки.

Під час підготовки оцінки Комісія повинна:

а) враховувати вплив заходів на виробників або постачальників таких продуктів ІКТ, послуг ІКТ або процеси ІКТ та на користувачів з точки зору вартості цих заходів та соціальних або економічних вигод, що випливають із очікуваного підвищеного рівня безпеки для цільові продукти ІКТ, послуги ІКТ або процеси ІКТ;

б) враховувати існування та імплементацію відповідного законодавства держав-членів та третіх країн;

в) провести відкритий, прозорий та всеохоплюючий процес консультацій з усіма відповідними зацікавленими сторонами та державами-членами;

г) враховувати будь-які терміни впровадження, перехідні заходи та періоди, зокрема щодо можливого впливу заходу на виробників або постачальників ІКТ-продуктів, ІКТ-послуг чи ІКТ-процесів, включаючи МСП;

д) запропонувати найшвидший та найефективніший спосіб реалізації переходу від добровільних до обов'язкових схем сертифікації.

Акредитовані Національним агентством з акредитації України (НААУ)

ООВ в Україні видають європейські сертифікати кібербезпеки, посилаючись на рівень забезпечення "базовий" або "суттєвий" на основі критеріїв, включених до європейської схеми сертифікації кібербезпеки, прийнятої Комісією.

В належним чином обґрунтованих випадках європейська схема сертифікації кібербезпеки може передбачати, що європейські сертифікати кібербезпеки, що виникають із цієї схеми, повинні видаватися в Україні лише національним органом. Такий орган повинен бути одним із наступних:

а) національний орган із сертифікації кібербезпеки України;

б) державний орган, який акредитований як ООВ в НААУ.

Якщо європейська схема сертифікації кібербезпеки вимагає рівня довіри „високий”, європейський сертифікат кібербезпеки за цією схемою в Україні повинен видавати лише національний орган із сертифікації кібербезпеки або, у наступних випадках, оцінка відповідності:

а) за попереднім схваленням національного органу з сертифікації кібербезпеки України для кожного окремого європейського сертифіката кібербезпеки, виданого ООВ;

б) на основі загального делегування завдання видачі таких європейських сертифікатів кібербезпеки ООВ національним органом з сертифікації кібербезпеки України.

Фізична або юридична особа, яка подає продукцію ІКТ, послуги ІКТ або процеси ІКТ на сертифікацію, надає доступ до всієї інформації, необхідної для проведення сертифікації, національного органу з сертифікації кібербезпеки України, де цей орган є органом, що видає європейський сертифікат кібербезпеки, або акредитованому в НААУ ООВ.

Власник європейського сертифіката кібербезпеки інформує уповноважений орган про будь-які виявлені згодом уразливості або порушення щодо безпеки сертифікованого ІКТ-продукту, послуги ІКТ чи процесу ІКТ, які можуть вплинути на його відповідність вимоги, що стосуються сертифікації. Цей орган передає цю інформацію без зайвої затримки відповідному національному органу з сертифікації кібербезпеки України.

Європейський сертифікат кібербезпеки видається на період, передбачений європейською схемою сертифікації кібербезпеки, і може бути продовжений за умови, що відповідні вимоги продовжують виконуватися й визнається в Україні.

Національні схеми сертифікації кібербезпеки в Україні та відповідні процедури для продуктів ІКТ, послуг ІКТ та процесів ІКТ, на які поширюється європейська схема сертифікації кібербезпеки, перестають мати наслідки з дати, встановленої в імплементаційний акт. Національні схеми сертифікації кібербезпеки в Україні та відповідні процедури для продуктів ІКТ, послуг ІКТ та процесів ІКТ, на які не поширюється європейська схема сертифікації кібербезпеки, повинні продовжувати існувати.

Україна не повинна запроваджувати нові національні схеми сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ, які вже охоплені європейською системою сертифікації кібербезпеки, яка діє.

Існуючі сертифікати, видані в рамках національних схем сертифікації кібербезпеки України та охоплених європейською схемою сертифікації кібербезпеки, залишаються чинними до дати закінчення терміну їх дії.

З метою уникнення роздробленості внутрішнього ринку Україна повідомляє Комісію та ECCG про будь-який намір скласти нові національні схеми сертифікації кібербезпеки України.

2.5 Призначення та експертна оцінка національного органу з сертифікації кібербезпеки України

Україна може призначити на своїй території один або декілька національних органів з сертифікації кібербезпеки України або, за згодою іншої держави-члена, призначає один або кілька національних органів з сертифікації кібербезпеки, створених у цій іншій державі-члені, що відповідають за наглядові завдання в призначуючої держави-члена.

Україна повинна повідомляти Комісію про призначені національні органи з сертифікації кібербезпеки України. Якщо Україна призначить більше одного

органу, вона також інформує Комісію про завдання, покладені на кожен з цих органів.

Кожен національний орган з сертифікації кібербезпеки повинен бути незалежним від суб'єктів, які він контролює у своїй організації, рішеннях щодо фінансування, правовій структурі та прийнятті рішень.

Україна повинна забезпечити, щоб:

а) діяльність національних органів з сертифікації кібербезпеки України, що стосується видачі європейських сертифікатів кібербезпеки, була суворо відокремлена від їх наглядових органів діяльність, і що ця діяльність здійснюється незалежно одна від одної;

б) національні органи з сертифікації кібербезпеки України мали достатні ресурси для здійснення своїх повноважень та ефективного та ефективного виконання своїх завдань.

Доцільно, щоб національні органи з сертифікації кібербезпеки України брали активну, дієву та безпечну участь в ECCG.

Національні органи з сертифікації кібербезпеки України повинні:

а) контролювати та застосовувати правила моніторингу відповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам європейських сертифікатів кібербезпеки або заяв ЄС про відповідність, включаючи механізми, що демонструють постійну відповідність зазначеним вимогам кібербезпеки, виданих на відповідних територіях у співпраці з іншими відповідними органами нагляду за ринком;

б) контролювати дотримання та виконувати зобов’язання виробників або постачальників продуктів ІКТ, послуг ІКТ чи ІКТ-процесів, які встановлені на їх відповідних територіях та здійснюють самооцінку відповідності, і, зокрема, контролювати дотримання та виконувати зобов’язання таких виробників або постачальників та у відповідній європейській схемі сертифікації кібербезпеки;

в) активно допомагати та підтримувати НААУ у моніторингу та нагляді діяльності акредитованих ООВ;

г) здійснювати моніторинг та нагляд за діяльністю державних

акредитованих ООВ;

д) де це доречно, уповноважити акредитовані ООВ, обмежити, призупинити чи скасувати існуючий дозвіл, якщо ООВ порушують вимоги Регламенту ЄС) 2019/881 [3];

е) розглядати скарги фізичних або юридичних осіб щодо європейських сертифікатів кібербезпеки, виданих національними органами з сертифікації кібербезпеки України, або європейських сертифікатів кібербезпеки, виданих ООВ, або стосовно заяв ЄС про відповідність, і розслідує предмет таких скарг у належному обсязі та інформує скаржника про хід та результати розслідування протягом розумного періоду;

ж) співпрацювати з іншими національними органами з сертифікації кібербезпеки або іншими державними органами, в тому числі шляхом обміну інформацією про можливу невідповідність продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам Регламенту (ЄС) 2019/881 [3] або вимогам конкретних європейських схем сертифікації кібербезпеки;

з) відстежувати відповідні події в галузі сертифікації кібербезпеки;

и) надавати річний підсумковий звіт про діяльність, яка проводиться відповідно до підпунктів б), в) та г) в цій частині та пунктів, що нижче.

Національний орган із сертифікації кібербезпеки України повинен мати принаймні такі повноваження:

а) вимагати від акредитованих ООВ, власників європейських сертифікатів кібербезпеки та емітентів заяв ЄС про відповідність надавати будь-яку інформацію, необхідну для виконання своїх завдань;

б) проводити розслідування у формі аудитів акредитованих ООВ, власників європейських сертифікатів кібербезпеки та емітентів заяв ЄС про відповідність з метою перевірки їх відповідності цим повноваженням;

в) вжити відповідних заходів відповідно до національного законодавства України для забезпечення відповідності акредитованих ООВ, власників європейських сертифікатів кібербезпеки та емітентів заяв ЄС відповідності Регламенту (ЄС) 2019/881 або європейській схемі сертифікації кібербезпеки;

г) отримати доступ до приміщень будь-яких акредитованих ООВ або власників європейських сертифікатів кібербезпеки з метою проведення розслідувань відповідно до процесуального законодавства Союзу, України або держав-членів;

д) відкликати відповідно до національного законодавства України європейські сертифікати кібербезпеки, видані національними органами з сертифікації кібербезпеки, або європейські сертифікати кібербезпеки, видані акредитованими ООВ відповідно, якщо такі сертифікати не відповідають Регламенту (ЄС) 2019/881 [3] або Європейському схема сертифікації кібербезпеки;

е) накладати штрафи відповідно до національного законодавства України та вимагати негайного припинення порушень зобов'язань, встановлених Регламентом (ЄС) 2019/881.

Національні органи з сертифікації кібербезпеки держав-членів повинні співпрацювати між собою та з Комісією, зокрема, шляхом обміну інформацією, досвідом та передовою практикою щодо сертифікації кібербезпеки та технічних питань, що стосуються кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ.

З метою досягнення еквівалентних стандартів у всьому Союзі щодо європейських сертифікатів кібербезпеки та заяв ЄС про відповідність, національні органи з сертифікації кібербезпеки України підлягають експертній перевірці.

Партнерська перевірка проводиться на основі обґрунтованих та прозорих критеріїв та процедур оцінки, зокрема щодо структурних вимог, вимог до людських ресурсів та процесів, конфіденційності та скарг.

Експертна оцінка повинна оцінити [3]:

а) де це застосовно, чи суворо відокремлюється діяльність національних органів з сертифікації кібербезпеки, що стосується видачі європейських сертифікатів кібербезпеки , зазначених у пункті (a) статті 56 (5) та у статті 56 (6) Регламенту (ЄС) 2019/881, від їх наглядової діяльності, визначеної у статті 58 та чи здійснюється ця діяльність незалежно одна від одної;

б) процедури нагляду та забезпечення виконання правил моніторингу

відповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ європейським сертифікатам кібербезпеки відповідно до пункту (a) статті 58 (7) Регламенту (ЄС) 2019/881;

в) процедури моніторингу та забезпечення виконання зобов'язань виробників або постачальників продуктів ІКТ, послуг ІКТ чи процесів ІКТ відповідно до пункту (b) статті 58 (7) Регламенту (ЄС) 2019/881;

г) процедури моніторингу, дозволу та нагляду за діяльністю ООВ;

д) де це можливо, чи мають співробітники органів влади чи органів, які видають сертифікати на рівень довіри „високий” відповідно до статті 56 (6) Регламенту (ЄС) 2019/881, відповідним досвідом.

Партнерський огляд повинен проводитись принаймні двома національними органами з сертифікації кібербезпеки інших держав-членів та Комісією та проводитись принаймні раз на п’ять років. ENISA може брати участь у експертній оцінці.

Комісія може прийняти виконавчі акти, що встановлюють план експертної оцінки, що охоплює період, щонайменше, п'ять років, що встановлює критерії щодо складу групи експертної оцінки, методології, яка застосовуватиметься для експертної оцінки, та графіка, частота та інші пов’язані з цим завдання. Приймаючи ці виконавчі акти, Комісія належним чином враховує думки ECCG. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 66 (2) Регламенту (ЄС) 2019/881.

Результати експертних оглядів вивчаються ECCG, яка складає резюме, які можуть бути оприлюднені, і, де це необхідно, видає настанови або рекомендації щодо дій чи заходів, які мають бути вжиті зацікавленими суб'єктами.

2.6 Вимоги до акредитованих органів з оцінки відповідності в Україні

ООВ в Україні повинні бути акредитовані НААУ, призначеними відповідно до Регламенту (ЄС) № 765/2008 [7]. Така акредитація видається лише тоді, коли ООВ відповідає наступним вимогам.

ООВ повинен бути створений відповідно до національного законодавства України та мати правосуб'єктність.

ООВ повинен бути стороннім органом, який не залежить від організації або продуктів ІКТ, послуг ІКТ чи процесів ІКТ, які він оцінює.

Орган, який належить до бізнес-асоціації чи професійної федерації, що представляє підприємства, що беруть участь у проектуванні, виробництві, забезпеченні, складанні, використанні або технічному обслуговуванні ІКТ-продуктів, ІКТ-послуг чи ІКТ-процесів, які, за його оцінкою, може вважатися ООВ, за умови, що демонструється його незалежність та відсутність будь-якого конфлікту інтересів.

ООВ, їх керівництвом вищого рівня та особами, відповідальними за виконання завдань з оцінки відповідності, не повинні бути проектувальник, виробник, постачальник, монтажник, покупець, власник, користувач чи супровідник ІКТ-продукту, послуги ІКТ або процесу ІКТ. який оцінюється, або уповноважений представник будь-якої із цих сторін. Ця заборона не виключає використання оцінених продуктів ІКТ, які необхідні для діяльності ООВ, або використання таких продуктів ІКТ в особистих цілях.

ООВ, їх керівництво вищого рівня та особи, відповідальні за виконання завдань з оцінки відповідності, не повинні брати безпосередньої участі у проектуванні, виробництві чи будівництві, маркетингу, монтажі, використанні або обслуговуванні продуктів ІКТ, послуг ІКТ або Процеси ІКТ, які оцінюються або представляють сторони, які беруть участь у цій діяльності. ООВ, їх керівництво вищого рівня та особи, відповідальні за виконання завдань з оцінки відповідності, не повинні займатися жодною діяльністю, яка може суперечити їх незалежності суджень або добросовісності щодо їх діяльності з оцінки відповідності. Ця заборона застосовується, зокрема, до консультаційних послуг.

Якщо ООВ належить чи експлуатується державним органом чи установою, незалежність та відсутність будь-якого конфлікту інтересів повинні бути забезпечені між національним органом з сертифікації кібербезпеки та ООВ та повинні бути задокументовані.

ООВ повинні забезпечити, щоб діяльність їхніх дочірніх підприємств та субпідрядників не впливала на конфіденційність, об'єктивність або неупередженість їх діяльності з оцінки відповідності.

ООВ та їх персонал повинні проводити діяльність з оцінки відповідності з найвищим ступенем професійної доброчесності та необхідною технічною компетентністю у конкретній галузі, і не повинні мати жодного тиску та стимулів, які можуть вплинути на їх судження або результати оцінки відповідності діяльності, включаючи тиск та спонукання фінансового характеру, особливо щодо осіб чи груп осіб, зацікавлених у результатах цієї діяльності.

ООВ повинен бути спроможним виконувати всі завдання з оцінки відповідності, покладені на нього згідно з Регламентом (ЄС) 2019/881 [3], незалежно від того, чи виконує ці завдання сам ООВ або від його імені та під його відповідальність. Будь-який підряд або зовнішній персонал для консультацій із зовнішнім персоналом повинен бути належним чином задокументований, не повинен залучати посередників і підлягати письмовій угоді, що охоплює, серед іншого, конфіденційність та конфлікт інтересів. Відповідний ООВ несе повну відповідальність за виконані завдання.

У будь-який час та для кожної процедури оцінки відповідності та кожного типу, категорії або підкатегорії продуктів ІКТ, послуг ІКТ або процесів ІКТ ООВ повинен мати у своєму розпорядженні необхідне:

а) персонал з технічними знаннями та достатнім та належним досвідом для виконання завдань з оцінки відповідності;

б) описи процедур, відповідно до яких має проводитися оцінка відповідності, для забезпечення прозорості цих процедур та можливості їх відтворення. Він повинен запровадити відповідну політику та процедури, що розрізняють завдання, які він виконує як орган, про який повідомлено, та його інші види діяльності;

в) процедури виконання діяльності, які належним чином враховують розмір підприємства, сектор, в якому воно функціонує, його структуру, ступінь складності технології продукту ІКТ, послуги ІКТ чи процесу ІКТ, а також масу

або послідовний характер виробничого процесу.

ООВ повинен мати засоби, необхідні для відповідного виконання технічних та адміністративних завдань, пов'язаних з діяльністю з оцінки відповідності, і мати доступ до всього необхідного обладнання та обладнання.

Особи, відповідальні за проведення заходів з оцінки відповідності, повинні мати:

а) надійне технічне та професійне навчання, що охоплює всі заходи з оцінки відповідності;

б) задовільні знання вимог до оцінок відповідності, які вони проводять, та належні повноваження для проведення цих оцінок;

в) відповідні знання та розуміння застосовних вимог та стандартів тестування;

г) можливість складати сертифікати, записи та звіти, що демонструють, що проводились оцінки відповідності.

Необхідно гарантувати неупередженість ООВ, їх керівництва на найвищому рівні, осіб, відповідальних за проведення заходів з оцінки відповідності, та будь-яких субпідрядників.

Винагорода керівництву вищого рівня та особам, відповідальним за проведення заходів з оцінки відповідності, не повинна залежати від кількості проведених оцінок відповідності або від результатів цих оцінок.

ООВ повинні укласти страхування відповідальності, якщо Україна не несе відповідальність згідно зі своїм національним законодавством, або сама Україна несе безпосередню відповідальність за оцінку відповідності.

ООВ та його персонал, його комітети, його дочірні компанії, його субпідрядники та будь-який асоційований орган або персонал зовнішніх органів ООВ повинні зберігати конфіденційність та дотримуватися професійної таємниці щодо всієї інформації, отриманої при здійсненні їх відповідності завдання з оцінки згідно з Регламентом (ЄС) 2019/881 [3] або згідно з будь-яким положенням національного законодавства України, що вводить в дію Регламенту (ЄС) 2019/881, за винятком випадків, коли розкриття інформації вимагається

законодавством Союзу або держав-членів, на які поширюються дії таких осіб, і за винятком стосовно компетентних органів держав-членів у який здійснює його діяльність. Права інтелектуальної власності повинні бути захищені. ООВ відповідності повинен мати документально оформлені процедури щодо цих вимог. За винятком цих вимог, перелічені вимоги вище не повинні виключати обмін технічною інформацією та регулятивними настановами між ООВ та особою, яка подає заявку на сертифікацію або яка розглядає, чи подавати заявку на сертифікацію.

ООВ повинні діяти відповідно до набору послідовних, справедливих та розумних умов та умов, враховуючи інтереси МСП щодо плати.

ООВ повинні відповідати вимогам відповідного стандарту ДСТУ EN ISO/IEC 17065:2014 Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг (EN ISO/IEC 17065:2012, IDT) [9], який гармонізований згідно з Регламентом (ЄС) No 765/2008 щодо акредитації ООВ, що виконують сертифікацію продукції ІКТ, послуг ІКТ або процесів ІКТ, що викладено у третьому розділі цієї магістерської роботи.

ООВ повинні забезпечити, щоб випробувальні лабораторії, що використовуються для оцінки відповідності, відповідали вимогам стандарту ДСТУ ISO/IEC 17025:2017 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій (ISO/IEC 17025:2017, IDT), який гармонізований згідно з Регламентом (ЄС) No 765/2008 щодо акредитації в НААУ лабораторій, що проводять випробування.

Якщо європейський сертифікат кібербезпеки видається національним органом з сертифікації кібербезпеки України відповідно до пункту (a) статті 56 (5) та статті 56 (6) Регламенту (ЄС) 2019/881 [3], орган із сертифікації національного органу з сертифікації кібербезпеки має бути акредитований НААУ, призначеними відповідно до Регламенту (ЄС) № 765/2008 [7].

Якщо європейські схеми сертифікації кібербезпеки встановлюють конкретні або додаткові вимоги щодо технічної компетентності ООВ для оцінки вимог щодо кібербезпеки, національний орган із сертифікації кібербезпеки України

дозволяється виконувати завдання за такими схемами лише ООВ, які відповідають цим вимогам.

Акредитація в НААУ, призначеними відповідно до Регламенту (ЄС) №765/2008, видається ООВ максимум на п’ять років і може бути продовжена на тих самих умовах за умови, що ООВ все ще відповідає вище викладеним вимогам. Національні органи з акредитації вживають усіх відповідних заходів у розумний строк для обмеження, призупинення або відкликання акредитації ООВ, якщо умови для акредитації не виконуються або більше не виконуються, або коли відповідність орган з оцінки порушує відповідні вимоги.

Для кожної європейської схеми сертифікації кібербезпеки національний орган сертифікації кібербезпеки України повідомляє Комісію про ООВ, які були акредитовані НААУ та, де це можливо, уповноважені видавати європейські сертифікати кібербезпеки на визначених рівнях забезпечення. Національний орган з сертифікації кібербезпеки України повідомляють Комісію про будь-які подальші зміни до них без зайвої затримки.

Через рік після набрання чинності європейською схемою сертифікації кібербезпеки Комісія опублікує перелік ООВ, про які було повідомлено відповідно до цієї схеми, в Офіційному віснику Європейського Союзу .

Якщо Комісія отримує повідомлення після закінчення терміну, вона оприлюднює поправки до переліку повідомлених ООВ в Офіційному віснику Європейського Союзу протягом двох місяців з дати отримання це повідомлення.

Національний орган з сертифікації кібербезпеки України може подати до Комісії запит на вилучення ООВ, про який повідомив цей орган, зі списку. Комісія публікує відповідні зміни до цього списку в Офіційному віснику Європейського Союзу. Союзу протягом одного місяця з дати отримання запиту національного органу з сертифікації кібербезпеки України.

2.7 Шляхи розв‘язання проблем сертифікації в сфері кібербезпеки для інформаційних та телекомунікаційних технологій в Україні

Ухвалення Акту про кібербезпеку, а також єдиних в рамках ЄС схем сертифікацій з кібербезпеки дозволить значно поліпшити протидію кібератакам і захист даних. Також, єдині стандарти з кібербезпеки в усіх країнах ЄС значним чином сприятимуть розвитку Єдиного Цифрового Ринку в ЄС і довірі користувачів до цифрових послуг.

Це дозволить компаніям, які працюють на ринку ЄС та України, вирішити проблему сертифікації своїх продуктів ІКТ, послуг ІКТ або процесів ІКТ відповідно до Акту ЄС про кібербезпеку, а інженерам – розвивати експертизу в сфері кібербезпеки та захисту даних з урахуванням нововведень.

Акт ЄС про кібербезпеку несе також переваги для громадян і бізнесу. Нові правила допоможуть людям довіряти пристроям, які вони використовують кожен день, тому що вони можуть обирати між продуктами, такими як пристрої Інтернету речей, які підпають під загрози кібербезпеки.

Система сертифікації стане універсальним центром сертифікації кібербезпеки, що призведе до значної економії коштів для підприємств, яким в іншому випадку довелося б подавати заявки на отримання кількох сертифікатів в декількох країнах. Єдина сертифікація також усуне потенційні бар’єри для входу на ринок. Більш того, компанії будуть зацікавлені в інвестуванні в кібербезпеку своїх продуктів і перетворюють це в конкурентну перевагу.

Разом з тим, на сьогодні є потужні проблеми сертифікації в сфері кібербезпеки для ІКТ в Україні.

Суть її полягає в наступному. В сучасному суспільстві довіра та конкурентні переваги, в тому числі і для сертифікації кібербезпеки, досягаються шляхом її гармонізації з вимогами глобальної системи Інфраструктури якості, яка реалізується шляхом укладання багаторівневої низки відповідних Угод, як показано на рис 2.2.

В Україні на сьогодні відсутні органи з сертифікації/ООВ в сфері

кібербезпеки для ІКТ, діяльність яких охоплюється цією Глобальною системою.

Разом з тим, Україна на сьогодні має всі Угоди, показані на рис. 2.3, необхідні для застосування сертифікації з кібербезпеки ІКТ.

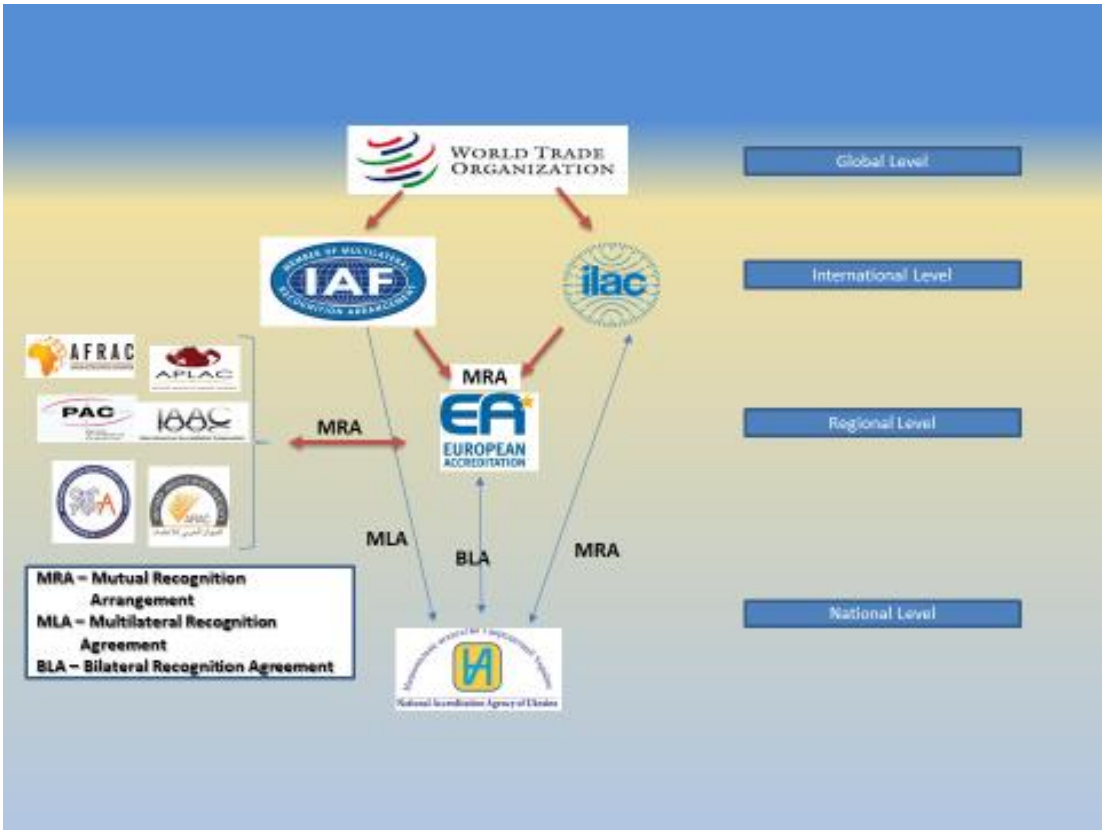

Рисунок 2.2 – Чотирьохрівнева Глобальна система Угод про визнання результатів сертифікації продукції, послуг та процесів

Таким чином, на внутрішньонаціональному рівні на сьогодні стає можливим застосування сертифікації з кібербезпеки ІКТ у спосіб, який дозволить такі сертифікації зробити визнаними в Глобальній Інфраструктурі якості.

Але, методологічно це потребує вирішення низки задач:

г) розробки схем сертифікації в сфері кібербезпеки ІКТ;

д) методичного забезпечення в сфері акредитації ООВ кібербезпеки ІКТ для НААУ;

е) забезпечення визнання результатів акредитації ООВ кібербезпеки ІКТ та сертифікації кібербезпеки ІКТ на глобальному (Європейському) рівнях.

International Accreditation Forum, Inc. (IAF)

Be it known that the

NATIONAL ACCREDITATION AGENCY OF UKRAINE (NAAU), UKRAINE

has been accepted as a Member of the

International Accreditation Forum, Inc.
Multilateral Recognition Arrangement

for the following:

Main Scope: Product Certification - ISO/IEC 17065 (16 August 2017)
Main Scope: Certification of Persons - ISO/IEC 17024 (16 August 2017)
Main Scope: Management System Certification - ISO/IEC 17021-1
Sub-Scopes: Level 5: ISO 9001 (16 August 2017)
Level 5: ISO 14001 (16 August 2017)

The Member on behalf of which this sheet is signed commits itself to comply with the requirements and obligations of Members of the IAF MLA.

Viktor Gorytskyy
Chairman,
National Accreditation Agency of Ukraine
DATE: 16 August 2017

Xiao Jianhua
Chairman,
International Accreditation Forum, Inc.
DATE: 16 August 2017

Рисунок 2.3 – Багатостороння Угода про визнання результатів сертифікації

2.8 Висновки з розділу 2

В розділі досліджено можливі шляхи вдосконалення національної системи кібербезпеки України в частині вирішення проблем сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС згідно Регламенту ЄС 2019/881, який почав діяти в Європейському Союзі з 2019 року.

Досліджені формалізовані цілі безпеки та рівні довіри для національних схем сертифікації кібербезпеки, процедури самооцінки відповідності та інші елементи схем сертифікації кібербезпеки, можливі для застосування в Національній системі кібербезпеки України.

При певній адаптації процедури призначення та експертної оцінки національного органу з сертифікації кібербезпеки можливі для застосування в національній системі кібербезпеки України, що визначено в законі України «Про кібербезпеку». А встановлені загальні вимоги до акредитованих ООВ в правовому

полі Україні можуть бути вимогами для органів з сертифікації кібербезпеки згідно вимог Регламенту ЄС 2019/881.

3 ПОРЯДОК АКРЕДИТАЦІЇ ОРГАНІВ З ОЦІНКИ ВІДПОВІДНОСТІ ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

3.1 Загальні вимоги до органу з оцінки відповідності інформаційних та телекомунікаційних технологій

3.1.1 Відповідальність за сертифікаційну діяльність

ООВ інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки є орган з сертифікації кібербезпеки продукції ІКТ, послуг ІКТ та процесів ІКТ, який у відповідності до вимог стандарту ДСТУ EN ISO/IEC 17065:2014 Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг (EN ISO/IEC 17065:2012, IDT) повинен бути юридичною особою або визначеною частиною юридичної особи, і таким чином нести юридичну відповідальність за всю свою сертифікаційну діяльність. [13]

Урядовий орган з сертифікації вважається юридичною особою на підставі його урядового статусу. [13]

Орган з сертифікації кібербезпеки повинен мати угоду, що має юридичну силу, для забезпечення сертифікаційної діяльності для своїх клієнтів. Сертифікаційні угоди повинні визначати відповідальність органу з сертифікації та його клієнтів. [13]

Орган з сертифікації кібербезпеки забезпечує, щоб сертифікаційна угода вимагала від клієнта відповідати, щонайменше, наступним вимогам:

а) клієнт завжди виконує визначені сертифікаційні вимоги, зокрема, вимоги до продукції ІКТ, послуг ІКТ та процесів ІКТ, які виконує клієнт як умову отримування або підтримування сертифікації, а також запроваджені відповідні зміни, що були повідомлені органом з сертифікації кібербезпеки.

Сертифікаційні вимоги охоплюють вимоги до клієнта, встановлені органом з сертифікації кібербезпеки згідно сертифікаційної угоди, і можуть також охоплювати вимоги до клієнта, встановлені схемою сертифікації.

Схема сертифікації – це система сертифікації/оцінювання відповідності, що

стосується певної продукції/послуги/процесу, до якої застосовують однакові встановлені вимоги, конкретні правила та процедури [10].

Вимоги до продукції ІКТ, послуг ІКТ та процесів ІКТ – це вимога, що безпосередньо пов'язана з продукцією/послугою/процесом та встановлена в стандартах або в інших нормативних документах як регламенти і технічні специфікації, визначених схемою сертифікації [9].

Такі сертифікаційні вимоги як укладання сертифікаційної угоди, оплата платежів, надавання інформації щодо змін у сертифікованих продуктах ІКТ, послугах ІКТ та процесах ІКТ, забезпечення доступу до сертифікованих продукції/послуг/процесів ІКТ під час діяльності з наглядання не є вимогами до продукції/послуг/процесів ІКТ;

б) якщо сертифікація застосовується до продукції ІКТ, що знаходиться в тривалому виробництві, то сертифікована продукція продовжує відповідати вимогам до неї;

в) клієнт запроваджує усі необхідні заходи для:

1) провадження оцінювання відповідності (відбирання та визначання) та наглядання (за потреби), зокрема, забезпечення документів та записів для розгляду і забезпечення доступу до відповідного устаткування, ділянок, підрозділів, персоналу та субпідрядників клієнта;

2) розгляду скарг;

3) участі спостерігачів, за потреби;

г) клієнт робить заяви щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ у відповідності до сфери сертифікації.

Сфера сертифікації – це ідентифікація:

1) продукції, процесів або послуг, для яких сертифікація надається;

2) застосовної схеми сертифікації;

3) стандарту(-ів) та іншого(-их) нормативного(-их) документу(-ів), зокрема, дати їх публікації, на відповідність яким оцінюють продукцію/процес/послугу [9];

д) клієнт не використовує сертифікацію продукції ІКТ, послуг ІКТ та

процесів ІКТ у такий спосіб, щоб зашкодити репутації органу з сертифікації кібербезпеки, і не робить будь-яких заяв щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, які орган з сертифікації кібербезпеки може розглядати як такі, що вводять в оману, або є несанкціонованими;

е) у випадку призупинення, скасування або закінчення терміну дії сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, клієнт припиняє використання всіх рекламних матеріалів, що містять будь-яке посилання на сертифікацію, і вживає заходів, які вимагає схема сертифікації (наприклад, повернення сертифікаційних документів), та виконує будь-які інші необхідні дії;

ж) якщо клієнт надає копії сертифікаційних документів іншим сторонам, документи повинні бути відтворені в їх цілісності або як це визначено схемою сертифікації;

з) посилаючись на сертифікацію своєї продукції ІКТ, послуги ІКТ та процесу ІКТ в засобах інформації, таких як документи, брошури чи рекламні матеріали, він виконує вимоги органу з сертифікації кібербезпеки або вимоги, визначені схемою сертифікації;

і) клієнт виконує усі вимоги, що можуть бути визначені схемою сертифікації щодо використання знаку відповідності та інформації стосовно продукції ІКТ, послуг ІКТ та процесів ІКТ;

и) клієнт зберігає записи щодо всіх відомих йому скарг, що стосуються відповідності сертифікаційним вимогам, та робить ці записи доступними органу з сертифікації кібербезпекит, за необхідності:

1) вживає відповідних заходів щодо таких скарг і будь-яких недоліків, виявлених у продукції ІКТ, послуг ІКТ та процесів ІКТ, що впливають на відповідність сертифікаційним вимогам;

2) документує виконані дії. Перевірка органом з сертифікації кібербезпеки цього пункту (и) може бути визначена схемою сертифікації;

к) клієнт невідкладно повідомляє органу з сертифікації кібербезпеки про зміни, які можуть вплинути на його здатність відповідати сертифікаційним вимогам. Приклади змін можуть охоплювати наступні області:

1) юридичний, комерційний, організаційний статус або право власності;

2) організація та керівництво (наприклад, ключові керівники, персонал, який приймає рішення, або технічний персонал);

3) модифікація продукції або виробничого процесу;

4) контактна адреса і виробничі площадки;

5) суттєві зміни в системі управління якістю.

Орган з сертифікації кібербезпеки повинен здійснювати контроль, як це визначено схемою сертифікації, за правом власності, використанням і демонструванням ліцензій, сертифікатів, знаків відповідності та будь-яких інших засобів для зазначення того, що продукція ІКТ, послуги ІКТ та процеси ІКТ є сертифікованими.

Керівництво щодо використання сертифікатів і знаків, дозволених органом з сертифікації, можна отримати в стандарті ISO/IEC Guide 23:1982 Methods of indicating conformity with standards for third-party certification systems [12].

Стандарт ДСТУ ISO/IEC 17030:2005 Оцінювання відповідності. Загальні вимоги до знаку відповідності третьої сторони (ISO/IEC 17030:2003, IDT) визначає вимоги для використання знаків третьої сторони.

В Україні будь-який акредитований ООВ може використовувати національний знак акредитації відповідно до опису та правил застосування національного знаку акредитації, затверджених Наказом Міністерства економіки та з питань європейської інтеграції України від 21.11.2002 №339 зареєстрованого у Міністерстві юстиції України 27.11.2002 №923/7211 та інструкції НААУ «Порядок використання знаків акредитації та посилання на акредитацію» (ІН-15.08.02, редакція 18 від 27.09.2019) [13].

Акредитованому органу з сертифікації кібербезпеки дозволяється використовувати національний знак акредитації разом з позначенням його реєстраційного номеру та стандарту ДСТУ EN ISO/IEC 17065, на відповідність якому орган було акредитовано.

Приклад використання національного знаку акредитації акредитованим ООВ показано на рис. 3.1.

Рисунок 3.1 – Приклад національного знаку акредитації

Знак IAF MLA (показано на рис. 3.2) можуть використовувати НААУ як підписант IAF MLA та ООВ, акредитовані НААУ. При використанні знаку IAF MLA НААУ та ООВ повинні додержуватись положень документа IAF ML 2 «Загальні принципи використання знаку IAF MLA».

У випадках некоректних посилань на схему сертифікації або оманливого використання ліцензій, сертифікатів, знаків чи будь-яких інших засобів для зазначення того, що продукція ІКТ, послуги ІКТ та процеси ІКТ є сертифікованими, виявлених у документації або в інших публічних засобах, необхідно вживати відповідних заходів.

Рисунок 3.2 – Приклад комбінованого знаку IAF MLA

Такі заходи визначені в стандарті ISO GUIDE 27:1983 Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity [12] і можуть охоплювати коригувальні дії, скасування сертифіката, публікацію щодо порушення і, за необхідності, дію юридичного характеру.

Орган з сертифікації кібербезпеки повинен мати відповідні заходи (наприклад, страхування або резервний фонд) для покриття зобов'язань, пов’язаних з його діяльністю, а також фінансову стабільність і ресурси, необхідні для його функціювання.

Політики і процедури, згідно з якими працює орган з сертифікації кібербезпеки та його адміністрація, повинні бути недискримінаційними. Процедури не можуть бути використані таким чином, щоб перешкоджати або ускладнювати доступ клієнтам. [13]

Орган з сертифікації кібербезпеки повинен робити свої послуги доступними для усіх клієнтів, чия діяльність підпадає до сфери його діяльності.

Доступ до процесу сертифікації не повинен залежати від розміру клієнта або членства в будь-якій асоціації чи групі, а сертифікація продукції ІКТ, послуг ІКТ та процесів ІКТ не повинна залежати від кількості вже виданих сертифікатів. Не повинно бути надмірних фінансових або інших умов.

Орган з сертифікації кібербезпеки може відмовити прийняти заявку або укласти договір на сертифікацію з клієнтом, якщо існують вагомі або явні причини, такі як участь клієнта в незаконній діяльності, клієнт має історію повторюваних невідповідностей до сертифікаційних вимог/ вимог до продукції ІКТ, послуг ІКТ та процесів ІКТ, або подібні питання, пов’язані з клієнтом. [13]

Орган з сертифікації кібербезпеки повинен обмежувати свої вимоги, оцінювання, аналізування, рішення і наглядання (якщо застосовуються) тими питаннями, які конкретним чином пов’язані зі сферою сертифікації.

3.1.2 Управління неупередженістю й конфіденційністю в процесі сертифікаційної діяльності

Орган з сертифікації кібербезпеки повинен здійснювати сертифікаційну діяльність неупереджено та нести відповідальність за неупередженість своєї сертифікаційної діяльності й не дозволяти комерційним, фінансовим або іншим впливам становити загрозу для неупередженості.

Орган з сертифікації кібербезпеки повинен на регулярній основі визначати ризики щодо своєї неупередженості, які включають ті ризики, що виникають в результаті його діяльності, його зв’язків, або зв’язків його персоналу. Проте, такі зв’язки не обов'язково являють собою ризик щодо неупередженості для органу з сертифікації кібербезпеки.

Зв’язки, які загрожують неупередженості органу з сертифікації кібербезпеки, можуть ґрунтуватися на правах власності, управлінні, персоналі, розподілених ресурсах, фінансах, контрактах, маркетингу (зокрема, торговій марці), а також на виплаті комісійної винагороди чи інших засобів стимулювання для залучення нових клієнтів тощо. [13]

Визначання ризиків не означає оцінку ризиків як описано в стандарті ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT).

Якщо ризик щодо неупередженості було ідентифіковано, орган з сертифікації кібербезпеки повинен бути здатним продемонструвати, як він усуває чи мінімізує такий ризик.

Орган з сертифікації кібербезпеки повинен мати зобов’язання вищого керівництва щодо неупередженості.

Орган з сертифікації кібербезпеки та будь-яка частина цієї ж юридичної особи та структурні підрозділи, що перебувають під його організаційним контролем, не повинні:

а) бути розробниками, виробниками, монтажниками, постачальниками сертифікованої продукції ІКТ або обслуговувати її;

б) бути конструкторами, розробниками, операторами сертифікованих процесів ІКТ або супроводжувати їх;

в) бути конструкторами, розробниками, постачальниками сертифікованих послуг ІКТ або супроводжувати їх;

г) пропонувати або надавати консультування своїм клієнтам;

д) пропонувати або надавати консультування своїм клієнтам щодо системи управління або проведення внутрішнього аудиту, якщо схема сертифікації вимагає оцінювання системи управління клієнта.

Консультування – це участь в:

а) розроблянні, виробництві, монтуванні, обслуговуванні або постачанні сертифікованої продукції або продукції, що підлягає сертифікації;

б) розроблянні, запроваджуванні, функціюванні або обслуговуванні сертифікованих процесів або процесів, що підлягають сертифікації;

в) розроблянні, запроваджуванні, надаванні або підтримуванні сертифікованих послуг або послуг, що підлягають сертифікації [9].

Зазначене вище не заважає наступному:

а) можливості обміну інформацією (наприклад, пояснення отриманих даних або роз’яснення вимог) між органом з сертифікації кібербезпеки та його клієнтами;

б) використанню, монтажу та супроводженню сертифікованих продукції ІКТ, послуг ІКТ та процесів ІКТ, що є необхідним для функціювання органу з сертифікації кібербезпеки.

Орган з сертифікації кібербезпеки повинен забезпечити, щоб діяльність сторонніх юридичних осіб, з якими взаємодіє орган з сертифікації кібербезпеки чи юридична особа, частиною якої він є, не компрометувала неупередженість його сертифікаційної діяльності. [13]

Якщо стороння юридична особа пропонує або виробляє сертифіковані продукцію ІКТ, послуги ІКТ та процеси ІКТ (зокрема, продукцію/послуги/процеси, що проходить сертифікацію) або пропонує чи надає консультування, керівний персонал органу з сертифікації кібербезпеки та персонал, залучений до

аналізування та процесу прийняття рішення щодо сертифікації, не повинен бути залученим до діяльності сторонньої юридичної особи. Персонал сторонньої юридичної особи не повинен бути залученим до керівництва органом з сертифікації кібербезпеки, аналізування або прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ.

Діяльність органу з сертифікації кібербезпеки не повинна проводитися на ринку або пропонуватися як діяльність, пов’язана з діяльністю організації, яка надає консультування. Орган з сертифікації кібербезпеки не повинен робити заяву або натякати, що сертифікація продукції ІКТ, послуг ІКТ та процесів ІКТ може бути простішою, легшою, швидшою або дешевшою, якщо буде залучена певна консалтингова організація.

В період, визначений органом з сертифікації кібербезпеки, персонал не можна залучати до аналізування або прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, стосовно якої вони надавали консультування.

Цей період може бути визначений в схемі сертифікації або, якщо його визначає орган з сертифікації кібербезпеки, він повинен бути достатнім для гарантування того, що процес аналізування або рішення проводились неупереджено. Зазвичай використовується період в два роки. [13]

Орган з сертифікації кібербезпеки повинен вжити заходів у відповідь на будь-які відомі йому ризики щодо його неупередженості, які є результатом дій інших осіб, органів або організацій.

Весь персонал органу з сертифікації кібербезпеки (як внутрішній так і зовнішній) або комітети, які можуть вплинути на сертифікаційну діяльність, повинні діяти неупереджено.

Орган з сертифікації кібербезпеки повинен нести відповідальність за зобов'язаннями, що мають юридичну силу, за управління усією інформацією, отриманої або створеної під час здійснення сертифікаційної діяльності. Уся інформація, за винятком тієї, що клієнт робить публічно доступною сам або за згодою між органом з сертифікації кібербезпеки і клієнтом (наприклад, з метою

відповіді на скаргу), розглядається як приватна інформація та повинна вважатися конфіденційною. Орган з сертифікації кібербезпеки повинен завчасно повідомити клієнта про те, яку інформацію він має намір зробити загальнодоступною. [13]

Якщо законодавство або договірні домовленості вимагають від органу з сертифікації кібербезпеки оприлюднити конфіденційну інформацію, клієнт або особа, яких це стосується, повинні бути повідомлені про це завчасно, якщо це не забороняється законом. [13]

Інформацію щодо клієнта, отриману від інших джерел, відмінних від клієнта (наприклад, від скаржника або регулятора), потрібно вважати конфіденційною.

Орган з сертифікації кібербезпеки повинен підтримувати (шляхом публікацій, через електронні носії інформації або в інший спосіб) та надавати на вимогу наступне:

а) інформацію (або посилання на неї) щодо схем сертифікації, зокрема, процедури оцінювання, правила та процедури для надавання і підтримування сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, розширення або скорочення сфери сертифікації, призупинення, скасування або відмови в сертифікації;

б) опис засобів, за допомогою яких орган з сертифікації кібербезпеки одержує фінансову підтримку, та загальну інформацію щодо оплати за послуги, що надаються заявникам та клієнтам;

в) опис прав та зобов’язань заявників та клієнтів, зокрема, вимоги, обмеження щодо використання назви органу з сертифікації кібербезпеки, знаку сертифікації та способів посилання на надану сертифікацію;

г) інформацію щодо процедур розгляду скарг та апеляцій.

3.2 Розробка вимог до структури та ресурсів органу з сертифікації кібербезпеки національної системи кібербезпеки України

3.2.1 Організаційна структура та механізм для забезпечення неупередженості

Для забезпечення неупередженості в органі з сертифікації кібербезпеки необхідно визначити структуру для сертифікаційної діяльності та управляти нею, зокрема задокументувати свою організаційну структуру, визначивши обов'язки, відповідальність і повноваження керівництва, а також іншого персоналу з сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ та будь-яких комітетів. Якщо орган з сертифікації кібербезпеки є визначеною частиною юридичної особи, структура повинна охоплювати розподіл повноважень та взаємозв'язки з іншими частинами в межах тієї ж юридичної особи.

Керівництво органу з сертифікації кібербезпеки повинне призначити раду, групу осіб чи особу, яка має усі повноваження та відповідальність щодо кожного з нижченаведеного:

а) розробляння політик, що стосуються функціювання органу з сертифікації кібербезпеки;

б) наглядання за впровадженням політик і процедур;

в) наглядання за фінансами органу з сертифікації кібербезпеки;

г) розробляння сертифікаційної діяльності;

д) розробляння сертифікаційних вимог;

е) оцінювання;

ж) аналізування;

з) рішення щодо сертифікації;

и) делегування, за потреби, повноважень комітетам або особам виконувати певну діяльність від його імені;

к) договірні умови;

л) забезпечення сертифікаційної діяльності відповідними ресурсами;

м) реагування на скарги та апеляції;

н) вимоги до компетентності персоналу;

о) система управління орану з сертифікації кібербезпеки.

Орган з сертифікації кібербезпеки повинен мати формальні правила для призначення, визначення повноважень і функціювання будь-яких комітетів, що залучають до процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ. Такі комітети повинні бути вільними від будь-яких комерційних, фінансових та інших тисків, які можуть вплинути на прийняття рішення. Орган з сертифікації кібербезпеки повинен підтримувати повноваження для призначення та відкликання членів таких комітетів.

Орган з сертифікації кібербезпеки повинен мати механізм для забезпечення своєї неупередженості. Такий механізм повинен підтримувати наступні вхідні дані [9]:

а) політики й принципи, що стосуються неупередженості його сертифікаційної діяльності;

б) будь-які тенденції в інтересах частини органу з сертифікації кібербезпеки, які дозволили б комерційним або іншим міркуванням перешкоджати послідовному неупередженому здійсненню сертифікаційної діяльності;

в) питання, що впливають на неупередженість та довіру до сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, зокрема, відкритість.

Інші завдання або обов’язки (наприклад, участь у процесі прийняття рішень щодо сертифікації) можуть бути встановлені в цьому механізмі, який буде забезпечувати, що ці додаткові завдання або обов’язки не компрометують його основну роль щодо забезпечення неупередженості.

Інші принципи для забезпечення довіри показано на рис. 3.3.

Можливим механізмом може бути комітет, створений одним чи декількома органами з сертифікації або запроваджений власником схеми, органом державної влади або рівноцінною стороною. [13]

Неупередженість

- Для забезпечення довіри до своєї діяльності та її результатів органи з сертифікації кібербезпеки та їх персонал повинні бути неупередженими і сприйматися як неупереджені.

Компетентність

- Компетентність персоналу, що підтримує система управління органу з сертифікації кібербезпеки, необхідна для надавання сертифікації, що забезпечує довіру.

•Конфіденційність та відкритість

- Управління балансом між вимогами щодо конфіденційності та відкритістю впливає на довіру зацікавлених сторін та їх усвідомлення цінності проведеної діяльності з оцінювання відповідності.

Реагування на скарги та апеляції

- Ефективне вирішення скарг та апеляцій є важливим засобом захисту органу з сертифікації кібербезпеки, його клієнтів та інших користувачів оцінювання відповідності від помилок, упущень або необґрунтованих дій. Довіра до діяльності з оцінювання відповідності зберігається, якщо скарги та апеляції розглядаються належним чином.

•Відповідальність

- За виконання вимог сертифікації несе відповідальність клієнт, а не орган з сертифікації кібербезпеки. Орган з сертифікації кібербезпеки несе відповідальність за отримання достатньої кількості об'єктивних доказів для прийняття рішення щодо сертифікації.

Рисунок 3.3 - Принципи для забезпечення довіри

Тому що, загальною метою сертифікації кібербезпеки є надання довіри всім зацікавленим сторонам, що продукція ІКТ, послуга ІКТ та процес ІКТ відповідає встановленим вимогам. Цінність сертифікації визначають рівнем суспільної довіри і впевненості, що створюється неупередженою і компетентною демонстрацією виконання встановлених вимог третьою стороною. Сторонами, які мають інтерес у сертифікації, можуть бути, але не обмежуються ними показано на рис. 3.4. [13]

Єдиний механізм для декількох схем сертифікації може задовольнити цю вимогу.

Механізм повинен бути формально задокументованим, щоб забезпечити наступне:

а) представництво основних зацікавлених сторін, збалансоване таким чином, що жоден окремий інтерес не переважає над іншими (внутрішній або зовнішній персонал органу з сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ вважається єдиним інтересом, і він не повинен переважати);

б) доступ до всієї інформації, необхідної для виконання всіх його функцій.

Рисунок 3.4 - Сторони, які мають інтерес у сертифікації кібербезпеки

Якщо вище керівництво органу з сертифікації кібербезпеки не підтримує вхідні дані для цього механізму, в механізмі повинна бути передбачена можливість вживати незалежні заходи (наприклад, інформування органів державної влади, органів з акредитації, зацікавлених сторін). Вживаючи відповідних заходів, необхідно виконати вимоги щодо конфіденційності стосовно клієнта та органу з сертифікації кібербезпеки. [13]

Не обов’язково вживати заходів щодо вхідних даних, що конфліктують з робочими процедурами органу з сертифікації кібербезпеки або іншими обов'язковими вимогами. Керівництво повинно задокументувати пояснення щодо рішення не підтримувати вхідні дані та зберігати документ для аналізування відповідним персоналом. [13]

Хоча не можливо представити усі інтереси в механізмі для забезпечення неупередженості, орган з сертифікації кібербезпеки повинен визначити та запросити ключові зацікавлені сторони.

Такими зацікавленими сторонами можуть бути клієнти органу з сертифікації кібербезпеки, замовники клієнтів, виробники, постачальники, користувачі, експерти з оцінювання відповідності, представники промислових торгівельних асоціацій, представники урядових регуляторних органів або інших

урядових структур, та представники неурядових організацій, зокрема, організацій споживачів. Може бути достатнім мати одного представника в механізмі від кожної зацікавленої сторони. [13]

Зазначені інтереси можуть бути обмежені залежно від характеру схеми сертифікації.

3.2.2 Вимоги до ресурсів органу з сертифікації кібербезпеки

Орган з сертифікації кібербезпеки повинен мати у штаті або можливість залучати достатню кількість персоналу для того, щоб забезпечити свою діяльність щодо схем сертифікації та застосовних стандартів і інших нормативних документів. [13]

Персонал охоплює штатних працівників органу з сертифікації кібербезпеки, а також осіб, які працюють за індивідуальними контрактами або угодами, що забезпечують управлінській контроль за ними та виконання ними систем/процедур органу з сертифікації кібербезпеки. [13]

Персонал повинен бути компетентним щодо функцій, які він виконує, зокрема, створення необхідних технічних висновків, розробляння та впровадження політик. [13]

Персонал, зокрема, члени комітетів, персонал зовнішніх органів, або персонал, який діє від імені органу з сертифікації кібербезпеки, повинен дотримуватись умов конфіденційності при поводженні з усією інформацією, отриманою або створеною під час виконання сертифікаційної діяльності, за винятком випадків, коли цього вимагає закон або схема сертифікації. [13]

Орган з сертифікації кібербезпеки повинен розробити, впровадити та підтримувати процедуру для управління компетентністю персоналу, залученого до процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ. Процедура повинна вимагати від органу з сертифікації кібербезпеки наступне:

а) визначити критерії компетентності персоналу для кожної функції в процесі сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, беручи до уваги

вимоги схем;

б) визначити потреби в навчання і забезпечити, за потреби, навчальні програми щодо процесів сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, вимог, методологій, видів діяльності та інших доречних вимог схем сертифікації;

в) продемонструвати, що персонал має необхідну компетентність відповідно до покладених на нього обов’язків та відповідальності;

г) формально уповноважувати персонал для виконання функцій в процесі сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ;

д) проводити моніторинг діяльності персоналу.

Орган з сертифікації кібербезпеки повинен підтримувати наступні записи щодо персоналу, який залучають до процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ [9]:

а) прізвище та адреса;

б) місце роботи та займана посада;

в) кваліфікація за освітою та фахова спеціальність;

г) досвід роботи та навчання;

д) оцінювання компетентності;

е) моніторинг діяльності;

ж) надані повноваження в рамках органу з сертифікації кібербезпеки;

з) дата останньої актуалізації кожного запису.

Орган з сертифікації кібербезпеки повинен вимагати від персоналу, залученого до процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, підписати контракт або інший документ, відповідно до якого він зобов'язується:

а) дотримуватися правил, визначених органом з сертифікації кібербезпеки, зокрема, тих, що стосуються конфіденційності та незалежності від комерційних та інших інтересів;

b) повідомляти про будь-який попередній та/або теперішній зв’язок від свого імені або від імені свого роботодавця з постачальником чи розробником продукції ІКТ, провайдером чи розробником послуг ІКТ, оператором чи розробником процесів ІКТ до оцінювання або сертифікації, на яке він був

призначений;

с) повідомити про будь-яку відому їм ситуацію, яка може створити конфлікт інтересів для них або для органу з сертифікації кібербезпеки.

Орган з сертифікації кібербезпеки повинен використовувати таку інформацію для ідентифікації загроз щодо неупередженості, яка виникає під час діяльності такого персоналу або організацій, в яких вони працюють.

Якщо орган з сертифікації кібербезпеки виконує діяльність з оцінювання, використовуючи власні внутрішні ресурси або інші ресурси під своїм безпосереднім контролем, така діяльність повинна відповідати застосовним вимогам відповідних міжнародних стандартів та інших документів, якщо це визначено схемою сертифікації. Для випробувань – вона повинна відповідати застосовним вимогам стандарту ДСТУ ISO/IEC 17025:2017 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій (ISO/IEC 17025:2017, IDT); для інспектування – вона повинна відповідати застосовним вимогам стандарту ДСТУ EN ISO/IEC 17020:2014 Оцінка відповідності. Вимоги до роботи різних типів органів з інспектування (EN ISO/IEC 17020:2012, IDT); для аудиту систем управління – вона повинна відповідати застосовним вимогам стандарту ДСТУ EN ISO/IEC 17021-1:2017 Оцінка відповідності. Вимоги до органів, які здійснюють аудит і сертифікацію систем управління. Частина 1. Вимоги (EN ISO/IEC 17021-1:2015, IDT; ISO/IEC 17021-1:2015, IDT). [13]

Необхідно завжди застосовувати вимоги до неупередженості персоналу з оцінювання, визначені у відповідному стандарті.

Нижче наведено приклади причин для випадків, коли деякі вимоги не застосовуються:

а) наявність в органі з сертифікації кібербезпеки досвіду використання результатів діяльності з оцінювання;

б) межі контролю органу з сертифікації кібербезпеки охоплюють випробовування (зокрема, спостереження за випробовуванням), інспектування (наприклад, визначення методів інспектування чи параметрів) або оцінювання системи управління (наприклад, вимагаються певні деталі системи управління);

в) окрема вимога еквівалентним чином міститься в стандарті ДСТУ EN ISO/IEC 17065, або не потрібна для підтримання довіри до рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ.

Орган з сертифікації кібербезпеки повинен передавати за субпідрядом діяльність з оцінювання тільки тим органам, які відповідають застосовним вимогам відповідних стандартів та інших документів, визначених схемою сертифікації. Для випробувань, такий орган повинен відповідати застосовним вимогам стандарту ДСТУ ISO/IEC 17025; для інспектування, такий орган повинен відповідати застосовним вимогам стандарту ДСТУ EN ISO/IEC 17020; для аудиту систем управління, він повинен відповідати застосовним вимогам стандарту ДСТУ EN ISO/IEC 17021-1.

Це може охоплювати субпідряд інших органів з сертифікації. Використовування зовнішнього персоналу за контрактом не є субпідрядом.

Якщо діяльність з оцінювання передається за субпідрядом органам, які не є незалежними (наприклад, лабораторіям клієнта), орган з сертифікації кібербезпеки повинен забезпечити управління діяльністю з оцінювання таким чином, щоб забезпечити довіру до результатів та наявність записів для підтвердження такої довіри. [13]

Орган з сертифікації кібербезпеки повинен мати угоду, що має юридичну силу, з органом, який надає послугу за субпідрядом. Ця угода повинна охоплювати положення щодо конфіденційності та конфлікту інтересів.

Орган з сертифікації кібербезпеки повинен:

а) нести відповідальність за всю діяльність, що була передана за субпідрядом іншому органу;

б) гарантувати, що орган, який надає послуги за субпідрядом, і персонал, який він використовує, не є залученими безпосередньо або через будь-якого іншого роботодавця таким чином, що може поставити під сумнів результати;

в) мати задокументовані політики, процедури та записи щодо кваліфікації, оцінювання та моніторингу всіх органів, які надають послуги за субпідрядом, що використовуються для сертифікаційної діяльності;

г) вести перелік затверджених постачальників послуг за субпідрядом;

д) впроваджувати коригувальні дії щодо будь-яких порушень контракту, що стали йому відомими;

е) заздалегідь інформувати клієнта щодо діяльності за субпідрядом для того, щоб надати клієнту можливість висловити заперечення. [13]

Якщо кваліфікацію, оцінювання та моніторинг органів, які надають субпідрядні послуги, оцінюють інші організації (наприклад, органи з акредитації, органи рівноправного оцінювання або урядові органи), орган з сертифікації кібербезпеки може брати до уваги результати такої кваліфікації та моніторингу за умови, що:

а) це визначено вимогами схеми;

б) сфера відповідає роботі, що виконується;

достовірність заходів щодо кваліфікації, оцінювання і моніторингу перевіряється з періодичністю, яку визначає орган з сертифікації кібербезпеки. [13]

3.3 Розробка процедур сертифікації інформаційних та телекомунікаційних технологій національної системи кібербезпеки України

Орган з сертифікації кібербезпеки може застосовувати одну або більшу кількість схем сертифікації, що охоплюють його сертифікаційну діяльність.

Елементи таких схем можуть бути поєднані з нагляданням за продукцією, або з оцінюванням та нагляданням за системою управління клієнта, або з обома.

Загальне керівництво щодо розробки схем надається в стандарті ДСТУ EN ISO/IEC 17067:2014 Оцінка відповідності. Основні положення сертифікації продукції та керівні вказівки щодо схем сертифікації продукції (EN ISO/IEC 17067:2013, IDT) з врахуванням вимог стандартів ДСТУ ISO/IEC Guide 28:2007. Оцінювання відповідності. Настанови щодо системи сертифікації продукції третьою стороною (ISO/IEC Guide 28:2004, IDT) та ДСТУ ISO/IEC Guide 53:2008. Порядок виконання системи управління якістю організації у сертифікації

продукції (ISO/IEC Guide 53:2005, IDT). [13]

Вимоги, на відповідність до яких оцінюються продукція ІКТ, послуги ІКТ та процеси ІКТ клієнта, повинні бути встановлені в конкретних стандартах та інших нормативних документах.

Керівництво для розробки відповідних нормативних документів міститься в стандарті ДСТУ ISO/IEC 17007:2009 Оцінювання відповідності. Настанови щодо складання нормативних документів, придатних до використання для оцінювання відповідності (ISO/IEC 17007:2009, IDT). [13]

Якщо потребуються пояснення щодо застосування документів для конкретної схеми сертифікації, вони повинні бути сформульовані відповідними неупередженими особами або комітетами, які мають необхідну технічну компетентність, і орган з сертифікації кібербезпеки повинен надавати їх на вимогу. [13]

3.3.1 Процес аналізування та розгляду заявки на сертифікацію інформаційних та телекомунікаційних технологій

При отриманні заявки орган з сертифікації кібербезпеки повинен отримати всю необхідну інформацію, щоб здійснити процес сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ згідно відповідної схеми сертифікації.

Прикладами необхідної інформації є наступні:

а) продукція ІКТ, послуги ІКТ та процеси ІКТ, що заявлені на сертифікацію;

б) стандарти та/або інші нормативні документи, на відповідність до яких буде проводитись сертифікація продукції ІКТ, послуг ІКТ та процесів ІКТ;

в) загальна характеристика клієнта, зокрема, назва та адреса місцезнаходження, суттєві аспекти його процесів і діяльності (якщо вимагається відповідною схемою сертифікації), і будь-які відповідні юридичні зобов'язання;

г) загальна інформація стосовно клієнта, яка є доречною для заявленої сфери сертифікації, як наприклад, види діяльності клієнта, його людські і технічні

ресурси, зокрема, лабораторії та/або засоби інспектування, його функції та взаємовідносини в більшій корпорації, якщо є;

д) інформація, що стосується всіх субпідрядних процесів, що використовує клієнт, яка впливає на відповідність до вимог; якщо клієнт визначив юридичну особу/осіб для виробництва сертифікованих продукції ІКТ, послуг ІКТ та процесів ІКТ, які є відмінні від клієнта, орган з сертифікації кібербезпеки може встановити на договірних засадах відповідні перевірки щодо такої юридичної особи/осіб, якщо це необхідно для ефективного наглядання; якщо такі перевірки на договірних засадах є необхідними, їх можна провести заздалегідь до надання офіційних документів щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ;

е) уся інша інформація, необхідна відповідно до доречних сертифікаційних вимог, зокрема, інформація для діяльності з початкового оцінювання та наглядання, наприклад, місця розташування виробництва сертифікованої продукції ІКТ та контактні особи на цих об’єктах. [13]

Щоб зібрати ці відомості, можна використовувати різноманітні засоби та механізми в різні проміжки часу, зокрема, форму заявки. Збирання такої інформації може проводитися в поєднанні з, або окремо від укладання обов'язкової до виконання сертифікаційної угоди. [13]

Заявка на розширення сфери сертифікації може охоплювати подібну продукцію, відмінні місця розташування тощо.

Орган з сертифікації кібербезпеки повинен провести розгляд отриманої інформації, щоб гарантувати, що:

а) інформація щодо клієнта та продукції ІКТ, послуг ІКТ та процесів ІКТ є достатньою для проведення процесу сертифікації;

б) будь-які відомі розбіжності у розумінні між органом з сертифікації кібербезпеки та клієнтом вирішені, зокрема, погодження щодо стандартів або інших нормативних документів;

в) заявлена сфера сертифікації визначена;

г) наявні засоби для виконання всіх видів діяльності з оцінювання;

д) орган з сертифікації кібербезпеки має компетентність і спроможність здійснювати сертифікаційну діяльність. [13]

Орган з сертифікації кібербезпеки повинен мати процес, щоб визначити, що запит клієнта щодо сертифікації охоплює:

а) тип продукції;

б) нормативний документ;

в) схему сертифікації, стосовно яких орган з сертифікації кібербезпеки не має попереднього досвіду.

Продукція може вважатися того ж самого типу, якщо знання вимог, характеристик і технології щодо однієї продукції, є достатніми для розуміння вимог, характеристик і технології іншої продукції. [13]

В таких випадках орган з сертифікації кібербезпеки повинен гарантувати, що він має компетентність і спроможність для усіх видів сертифікаційної діяльності, що необхідно виконати, і він зберігає записи щодо обґрунтування рішення провести сертифікацію. [13]

Орган з сертифікації кібербезпеки повинен відмовитися проводити конкретну сертифікацію, якщо йому не вистачає будь-якої компетентності або він не має спроможності провести таку сертифікаційну діяльність.

Якщо орган з сертифікації кібербезпеки не проводить будь-які види діяльності, покладаючись на сертифікації, які вже були надані даному клієнту або іншим клієнтам, тоді орган з сертифікації кібербезпеки повинен посилатися в своїх записах на вже існуючу сертифікацію. Якщо клієнт вимагає, орган з сертифікації кібербезпеки повинен забезпечити обґрунтування для виключення цих видів діяльності.

3.3.2 Процес оцінювання відповідності, аналізування даних та прийняття рішення щодо сертифікації інформаційних та телекомунікаційних технологій

Орган з сертифікації кібербезпеки повинен мати план для діяльності з оцінювання, щоб управляти необхідними заходами.

Залежно від особливостей схеми сертифікацій і вимог до продукції ІКТ, послуг ІКТ та процесів ІКТ, план може бути узагальненим, придатним для всіх видів діяльності, зокрема, оцінювання системи управління якістю, за необхідності, або конкретним планом для певного виду діяльності, або комбінацією обох варіантів. [13]

Орган з сертифікації кібербезпеки повинен призначати персонал для виконання кожного завдання з оцінювання, яке він виконує, використовуючи свої внутрішні ресурси. [13]

Завдання субпідряду виконує персонал, зазвичай призначений організацією, яка отримала завдання на субпідряд. Такий персонал зазвичай не призначається органом з сертифікації кібербезпеки. [13]

Орган з сертифікації кібербезпеки повинен забезпечити всю необхідну інформацію та/або зробити документацію доступною для виконання завдань з оцінювання.

Завдання з оцінювання можуть охоплювати такі дії як розгляд розробки та документації, відбирання зразків, випробовування, інспектування та аудит.

Орган з сертифікації кібербезпеки повинен виконувати діяльність з оцінювання, яку він здійснює з залученням своїх внутрішніх ресурсів, та повинен управляти ресурсами субпідряду у відповідності до плану з оцінювання. Необхідно оцінити продукцію ІКТ, послуги ІКТ та процеси ІКТ відповідно до вимог, які містить сфера сертифікації, та інших вимог, визначених схемою сертифікації.

Орган з сертифікації кібербезпеки повинен покладатися тільки на ті результати з оцінювання, що стосуються сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, завершеної до отримання заявки на сертифікацію, якщо він несе відповідальність за ці результати і пересвідчився, що орган, який виконував оцінювання, відповідає вимогам, що визначені схемою сертифікації. [13]

Цей процес може охоплювати роботи, що проводиться відповідно до угод про визнання між органами з сертифікації кібербезпеки.

Орган з сертифікації кібербезпеки повинен інформувати клієнта про всі

невідповідності.

Якщо виявлено одну або більше невідповідностей і клієнт висловлює зацікавленість в продовженні процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, орган з сертифікації кібербезпеки повинен надати інформацію щодо додаткового оцінювання, необхідного для перевіряння того, що невідповідності були усунені.

Якщо клієнт погоджує виконання додаткових завдань з оцінювання, необхідно повторити процес, щоб виконати додаткові завдання з оцінювання.

Результати усіх дій з оцінювання потрібно задокументувати до початку аналізування. [13]

Зазначена документація може забезпечити думку щодо того, чи виконуються вимоги до продукції ІКТ, послуг ІКТ та процесів ІКТ (зокрема, вимоги до системи управління якістю, в рамках якої продукція/послуга/процес виробляється, якщо вимагається схемою сертифікації). [13]

Схема сертифікації може визначати, чи оцінювання було проведено органом з сертифікації кібербезпеки під його відповідальністю, чи проведено до подання заявки на сертифікацію.

Орган з сертифікації кібербезпеки повинен призначити щонайменше одну особу для проведення аналізування всієї інформації і результатів оцінювання. Аналізування повинен виконувати персонал, який не був залучений до процесу оцінювання. [13]

Рекомендації для прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, засновані на аналізуванні, повинні бути задокументовані, якщо аналізування і прийняття рішення щодо сертифікації не виконувала одна й та сама особа. [13]

Орган з сертифікації кібербезпеки повинен нести відповідальність за рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ та повинен підтримувати повноваження щодо їх прийняття.

Орган з сертифікації кібербезпеки повинен призначити принаймні одну особу для прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та

процесів ІКТ на основі усієї інформації, отриманої в процесі оцінювання, її аналізування, а також будь-якої іншої доречної інформації. Рішення щодо сертифікації повинна приймати особа або група осіб, які не були залучені до процесу оцінювання.

Аналізування даних і прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ можуть виконувати одночасно одна й та сама особа або група осіб.

Особа або особи, призначені органом з сертифікації кібербезпеки приймати рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, повинні працювати на постійній основі в або за контрактом з:

а) органом з сертифікації кібербезпеки;

б) організацією, що знаходиться під організаційним контролем органу з сертифікації кібербезпеки.

Організаційний контроль органу з сертифікації кібербезпеки може бути одним з наступних:

а) органу з сертифікації кібербезпеки належить повна власність або більша частина власності іншої організації;

б) органу з сертифікації кібербезпеки належить більшість в раді директорів іншої організації;

в) орган з сертифікації кібербезпеки має задокументовані повноваження щодо управління іншою організацією в мережі юридичних осіб (до якої орган з сертифікації належить), пов’язаної правом власності або радою директорів.

Для урядових органів з сертифікації, інші частини того ж самого урядового органу можуть вважатися такими, що «пов’язані правом власності» з органом з сертифікації.

Особи, що працюють в штаті або за контрактом з організаціями, що знаходяться під організаційним контролем, повинні відповідати тим самим вимогам стандарту ДСТУ EN ISO/IEC 17065, що і особи, що працюють в штаті або за контрактом з органом з сертифікації кібербезпеки. [13]

Орган з сертифікації кібербезпеки повинен повідомити клієнту про своє

рішення не надавати сертифікацію та повинен визначити причини для цього рішення. [13]

Якщо клієнт виявляє зацікавленість в продовженні процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, орган з сертифікації кібербезпеки може відновити процес оцінювання. [13]

3.3.3 Процес підтримання та зберігання записів за результатами сертифікації інформаційних та телекомунікаційних технологій

Орган з сертифікації кібербезпеки повинен надати клієнту офіційні документи щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, які чітко визначають або дозволяють ідентифікувати наступне:

а) назву та адресу органу з сертифікації кібербезпеки;

б) дату надання сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ (дата не повинна передувати даті прийняття рішення щодо сертифікації);

в) назву та адресу клієнта;

г) сферу сертифікації. Якщо стандарт або інший нормативний документ, на відповідність до яких сертифікація проводиться, містить посилання на інші стандарти або нормативні документи, їх не обов’язково включати в офіційні документи щодо сертифікації;

д) термін дії або дату закінчення сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, якщо дія сертифікації закінчується після встановленого періоду часу;

е) будь-яку іншу інформацію, яку вимагає схема сертифікації.

Офіційні документи щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ повинні містити підпис та іншу визначену авторизацію особи або осіб органу з сертифікації кібербезпеки, які мають такі повноваження.

Ім’я та посада особи, яка несе відповідальність за документи щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, зареєстровані в органі з сертифікації кібербезпеки, є прикладом "визначеної авторизації" окрім підпису.

Офіційні документи щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ потрібно надавати одночасно або після того як:

а) рішення надати або розширити сферу сертифікації було прийнято;

б) сертифікаційні вимоги виконані;

в) сертифікаційна угода складена/підписана.

Орган з сертифікації повинен підтримувати інформацію щодо сертифікованої продукції ІКТ, послуг ІКТ та процесів ІКТ, яка містить, щонайменше, наступне:

а) ідентифікацію продукції ІКТ, послуг ІКТ та процесів ІКТ;

б) стандарти та інші нормативні документи, на відповідність до яких продукція ІКТ, послуга ІКТ та процес ІКТ сертифіковано;

в) ідентифікацію клієнта.

Необхідність робити публічною або надавати за запитом частину інформації з реєстру (за допомогою публікацій, електронних або інших засобів) визначається відповідною схемою. Щонайменше, орган з сертифікації кібербезпеки повинен надавати за запитом інформацію щодо чинності наданої сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ. [13]

Якщо орган з сертифікації кібербезпеки надає інформацію до схеми, реєстр схеми повинен забезпечити виконання зазначеної вимоги.

Орган з сертифікації кібербезпеки повинен зберігати записи, щоб продемонструвати, що всі вимоги до процесу сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ (вимоги стандарту ДСТУ EN ISO/IEC 17065 та схеми сертифікації) були виконані ефективно.

Орган з сертифікації кібербезпеки повинен зберігати записи в умовах конфіденційності.

Записи необхідно перевозити, передавати і пересилати тільки у спосіб, що забезпечує дотримання умов конфіденційності.

Якщо схема сертифікації передбачає проведення повторного оцінювання продукції ІКТ, послуг ІКТ та процесів ІКТ в межах визначеного циклу, записи необхідно зберігати, щонайменше, для поточного і попереднього циклу

сертифікації. Інакше, записи необхідно зберігати в період, визначений органом з сертифікації кібербезпеки.

Для визначення часу збереження можна брати до уваги юридичні умови та угоди щодо визнання. [13]

3.3.4 Процес наглядання за сертифікованими інформаційними та телекомунікаційними технологіями та впровадження змін

Якщо схема сертифікації кібербезпеки вимагає наглядання, орган з сертифікації кібербезпеки повинен започаткувати наглядання за продукцією ІКТ, послугою ІКТ та процесом ІКТ, охопленою рішенням щодо сертифікації, згідно зі схемою сертифікації.

Стандарт ДСТУ EN ISO/IEC 17067 надає приклади діяльності з наглядання в схемах сертифікації.

Критерії та процес для діяльності з наглядання визначає кожна схема сертифікації.

У разі необхідності, при нагляданні здійснити процес оцінювання, аналізування даних або прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ.

Якщо постійне використання знаку сертифікації було дозволено для розміщення на продукції ІКТ типу (або його упаковці), що була сертифікована, необхідно встановити та визначити періодичну діяльність з наглядання маркованої продукції, щоб забезпечити постійну демонстрацію виконання вимог до продукції ІКТ.

Якщо постійне використання знаку сертифікації було дозволено для процесу або послуги ІКТ, необхідно встановити та визначити періодичну діяльність з наглядання, щоб забезпечити постійну демонстрацію виконання вимог до процесу або послуги ІКТ. [13]

Якщо схема сертифікації вводить нові або змінені вимоги, що впливають на клієнта, орган з сертифікації кібербезпеки повинен забезпечити, щоб всі зміни

були повідомлені всім клієнтам. Орган з сертифікації кібербезпеки повинен перевірити впровадження змін клієнтами та вжити заходів, які вимагає схема сертифікації.

Для забезпечення виконання цих вимог, можуть бути необхідні договірні угоди з клієнтами. Модель ліцензійної угоди щодо використання сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, зокрема, аспекти щодо повідомлення змін, за потреби, надаються в стандарті ДСТУ ISO/IEC Guide 28, Додаток Е.

Орган з сертифікації кібербезпеки повинен брати до уваги інші зміни, що впливають на сертифікацію продукції ІКТ, послуг ІКТ та процесів ІКТ, зокрема, зміни, розпочаті клієнтом, та повинен визначати відповідну дію.

Зміни, що впливають на сертифікацію продукції ІКТ, послуг ІКТ та процесів ІКТ, можуть охоплювати нову інформацію, що стосується виконання сертифікаційних вимог, отримані органом з сертифікації кібербезпеки після того, як сертифікація була надана.

Дії щодо впровадження змін, що впливають на сертифікацію продукції ІКТ, послуг ІКТ та процесів ІКТ, повинні охоплювати, за потреби, наступне:

а) оцінювання;

б) аналізування даних, отриманих під час оцінювання;

в) прийняття рішення;

г) видання змінених офіційних документів щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ для розширення або скорочення сфери сертифікації;

д) видання документів щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ щодо змін в діяльності з наглядання (якщо наглядання є частиною схеми сертифікації).

Записи щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ повинні містити обґрунтування для виключення будь-яких із згаданих вище видів діяльності (наприклад, якщо змінена сертифікаційна вимога не є зміною вимоги до продукції, та діяльність з оцінювання, аналізування даних і прийняття рішення не потрібна). [13]

3.3.5 Закінчення терміну дії, скорочення, призупинення або скасування сертифікації інформаційних та телекомунікаційних технологій

Якщо за результатами наглядання або іншим чином була виявлена невідповідність до сертифікаційних вимог, орган з сертифікації кібербезпеки повинен розглянути та прийняти рішення щодо відповідних дій.

Відповідні дії можуть охоплювати наступне:

а) продовження дії сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ за умови, визначеної органом з сертифікації кібербезпеки (наприклад, позаплановий нагляд);

б) скорочення сфери сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, щоб вилучити невідповідні види продукції;

в) призупинення сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ на період проведення клієнтом коригувальних заходів;

г) скасування сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ.

У разі необхідності, здійснити процес оцінювання, аналізування даних та прийняття рішення щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ.

Якщо сертифікація продукції ІКТ, послуг ІКТ та процесів ІКТ зупиняється (за запитом клієнта), призупиняється або скасовується, орган з сертифікації кібербезпеки повинен вжити заходів, визначених схемою сертифікації, і внести всі необхідні зміни до офіційних документів щодо сертифікації, публічної інформації, дозволів щодо використання знаків тощо, для того, щоб забезпечити унеможливлення посилання на те, що продукція/послуга/процес залишається сертифікованою. Якщо сфера сертифікації скорочується, орган з сертифікації кібербезпеки повинен вжити заходів, визначених схемою сертифікації, і внести усі необхідні зміни до офіційних документів щодо сертифікації, публічної інформації, дозволів щодо використання знаків тощо, для того, щоб забезпечити, що про скорочену сферу явним чином було повідомлено клієнту і чітко визначено в офіційних документів щодо сертифікації та у публічній інформації. [13]

Якщо сертифікація призупинена, орган з сертифікації кібербезпеки повинен призначити одну особу або більшу кількість персоналу, щоб сформулювати та повідомити клієнту наступне:

а) дії, необхідні для закінчення призупинення і поновлення сертифікації для продукції ІКТ, послуг ІКТ та процесів ІКТ відповідно до схеми сертифікації;

б) будь-які інші дії, що вимагає схема сертифікації.

Зазначений персонал повинен бути компетентним щодо знань та розуміння усіх аспектів поводження з призупиненими сертифікатами.

У разі необхідності здійснити процес оцінювання, аналізування даних або прийняття рішення, що є необхідними для рішення щодо призупинення сертифікації або тих дій, яких вимагає схема сертифікації.

Якщо сертифікація була поновлена після призупинення, орган з сертифікації кібербезпеки повинен внести всі необхідні зміни до офіційних документів щодо сертифікації, публічної інформації, дозволів щодо використання знаків тощо, щоб забезпечити наявність усіх відповідних посилань на те, що продукція ІКТ, послуга ІКТ та процес ІКТ продовжують бути сертифікованими. Якщо рішення скоротити сферу сертифікації було прийнято як умова поновлення, орган з сертифікації кібербезпеки повинен внести всі необхідні зміни до офіційних документів щодо сертифікації, публічної інформації, дозволів щодо використання знаків тощо для забезпечення того, що про скорочену сферу сертифікації явним чином було повідомлено клієнту та чітко визначено у офіційних документів щодо сертифікації та в публічній інформації. [13]

3.3.6 Процес розгляду скарг та апеляцій

Орган з сертифікації кібербезпеки повинен мати задокументований процес для отримання, оцінювання та прийняття рішень щодо скарг та апеляцій. Орган з сертифікації кібербезпеки повинен реєструвати та відстежувати скарги та апеляції, а також дії, що виконуються для їх вирішення. [13]

На рис.3.5 Показана схема процесу розгляду скарг та апеляцій.

Рисунок 3.5 – Схема процесу розгляду скарг та апеляцій

Після отримання скарги або апеляції, орган з сертифікації кібербезпеки повинен визначити, чи скарга або апеляція стосується сертифікаційної діяльності, за яку він відповідає, і якщо так, повинен розглянути її. [13]

Орган з сертифікації кібербезпеки повинен підтвердити отримання офіційної скарги або апеляції.

Орган з сертифікації кібербезпеки повинен нести відповідальність за збирання і перевірку всієї необхідної інформації (до можливого ступеня), щоб прийняти рішення щодо скарги або апеляції.

Рішення за результатами розгляду скарги або апеляції повинні приймати або її аналізування та затвердження повинні проводити особи, що не були залучені до сертифікаційної діяльності, пов'язаної зі скаргою або апеляцією.

Щоб забезпечити відсутність конфлікту інтересів, для розгляду або прийняття рішення щодо скарги або апеляції, орган з сертифікації кібербезпеки не повинен залучати персонал (зокрема, тих, хто має керівну посаду), хто надав консультування клієнту або працював у нього впродовж двох років після надання консультування або закінчення роботи у клієнта. [13]

Орган з сертифікації кібербезпеки повинен як найшвидше надати скаржнику офіційне повідомлення щодо результатів та завершення процесу розгляду скарги.

Орган з сертифікації кібербезпеки повинен надати апелянту офіційне повідомлення щодо результатів та завершення процесу розгляду апеляції.

Орган з сертифікації кібербезпеки повинен вжити будь-яких подальших заходів, необхідних для вирішення апеляції або скарги.

3.4 Розробка процедур системи управління органу з сертифікації кібербезпеки національної системи кібербезпеки України

Орган з сертифікації повинен встановити та підтримувати систему управління, здатну досягти узгодженого виконання вимог стандарту ДСТУ EN ISO/IEC 17065.

Система управління органу з сертифікації кібербезпеки повинна охоплювати наступне:

а) загальну документацію системи управління (наприклад, настанова, політики, визначення відповідальності;

б) управління документами;

в) управління записами;

г) аналізування з боку керівництва;

д) внутрішній аудит;

е) коригувальні дії;

ж) запобіжні дії.

Вище керівництво органу з сертифікації кібербезпеки повинно розробити, задокументувати і підтримувати політики та цілі для виконання стандарту ДСТУ EN ISO/IEC 17065 та схеми сертифікації, а також забезпечити, щоб політики та цілі були усвідомлені та впроваджені на всіх рівнях організації органу з сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ.

Вище керівництво органу з сертифікації кібербезпеки повинно надавати докази виконання своїх зобов'язань щодо розробляння та впровадження системи управління та її ефективності в досягненні узгодженого виконання стандарту ДСТУ EN ISO/IEC 17065.

Вище керівництво органу з сертифікації кібербезпеки повинне призначити представника керівництва, який незалежно від інших обов'язків, повинен мати відповідальність та повноваження, які включають:

а) забезпечення того, що процеси і процедури, необхідні для системи управління, розроблені, впроваджені та підтримуються;

б) звітування вищому керівництву щодо функціювання системи управління і будь-якої потреби щодо поліпшення.

Усі документи, процеси, системи, записи тощо щодо виконання вимог стандарту ДСТУ EN ISO/IEC 17065, повинні бути включені до, посилатися на або бути пов'язані з документами системи управління.

Весь персонал, залучений до сертифікаційної діяльності, повинен мати доступ до частин документів системи управління та пов'язаної інформації, які застосовні до їх обов'язків. [13]

3.4.1 Процедура управління документами та записами органу з сертифікації кібербезпеки

Орган з сертифікації кібербезпеки повинен розробити процедури для управління документами (внутрішніми та зовнішніми), які стосуються виконання стандарту ДСТУ EN ISO/IEC 17065.

Процедури повинні визначати засоби контролю, необхідні для:

а) затвердження документів на відповідність перед їх введенням в дію;

б) перегляду і актуалізації (за потреби) та повторного затвердження документів;

в) забезпечення ідентифікації змін і стану поточного перегляду документів;

г) забезпечення наявності відповідних версій застосовних документів в місцях їх використання;

д) забезпечення розбірливості та простоти ідентифікації документів;

е) забезпечення ідентифікації документів зовнішнього походження та контролю їх розповсюдження;

ж) запобігання ненавмисного використовування застарілих документів, і застосовування належної їх ідентифікації, якщо вони зберігаються з будь-якої метою.

Документи можуть бути в будь-якій формі або на будь-яких видах носіїв.

Орган з сертифікації кібербезпеки повинен встановити процедури для визначення засобів контролю, необхідних для ідентифікації, зберігання, захисту, відновлювання, забезпечення терміну зберігання і розміщення записів, пов'язаних з виконанням стандарту ДСТУ EN ISO/IEC 17065.

Орган з сертифікації кібербезпеки повинен встановити процедури для збереження записів протягом періоду, який відповідає договірним та юридичним зобов'язанням.

Доступ до цих записів повинен відповідати заходам щодо забезпечення умов конфіденційності.

3.4.2 Процедура аналізування з боку керівництва органу з сертифікації кібербезпеки

Вище керівництво органу з сертифікації кібербезпеки повинне встановити процедури для аналізування систему управління в заплановані інтервали часу для забезпечення її постійної придатності, відповідності та ефективності, зокрема, аналізування заявлених політик та цілей, що стосуються виконання стандарту ДСТУ EN ISO/IEC 17065. [13]

Такі аналізування потрібно проводити щонайменше один раз на рік.

Альтернативою може бути повне аналізування, що розбивається на елементи, яке потрібно завершити за період в 12 місяців. Необхідно зберігати записи щодо аналізування з боку керівництва.

Вхідні дані для аналізування з боку керівництва повинні охоплювати інформацію щодо:

а) результатів внутрішніх і зовнішніх аудитів;

б) зворотного зв'язку від клієнтів і зацікавлених сторін, що стосуються

виконання стандарту ДСТУ EN ISO/IEC 17065. Зацікавлені сторони можуть включати власників схеми;

в) зворотного зв'язку від механізму, що забезпечує неупередженість;

г) статусу запобіжних і коригувальних дій;

д) подальших дій за результатами попереднього аналізування з боку керівництва;

е) досягнення цілей;

ж) змін, які можуть вплинути на систему управління;

з) апеляцій та скарг.

Вихідні дані аналізування з боку керівництва повинні охоплювати рішення та дії щодо:

а) поліпшення ефективності системи управління та її процесів;

б) удосконалення органу з сертифікації кібербезпеки щодо виконання стандарту ДСТУ EN ISO/IEC 17065;

в) необхідних ресурсів. [13]

3.4.3 Процедура проведення внутрішніх аудитів органу з сертифікації кібербезпеки

Орган з сертифікації кібербезпеки повинен встановити процедури для внутрішніх аудитів, щоб перевірити, чи виконує він вимоги стандарту ДСТУ EN ISO/IEC 17065 і система управління ефективно впроваджена та підтримується.

Стандарт ДСТУ ISO 19011:2019 Настанови щодо проведення аудитів систем управління (ISO 19011:2018, IDT) забезпечує керівництво щодо проведення внутрішніх аудитів.

Програму аудиту потрібно складати, враховуючи важливість процесів та областей, що підлягають аудиту, а також результати попередніх аудитів.

Зазвичай внутрішні аудити потрібно проводити щонайменше один раз кожні 12 місяців або завершити за період в 12 місяців для сегментованих внутрішніх аудитів. Зміни (зменшення або відновлення) частоти внутрішніх

аудитів або інтервалу часу, за який внутрішні аудити потрібно завершити, повинні бути результатом задокументованого процесу прийняття рішення. Такі зміни повинні ґрунтуватися на відносній стабільності та постійній ефективності системи управління. Необхідно підтримувати записи щодо рішень про зміни частоти проведення внутрішніх аудитів або інтервалу часу, за який вони будуть завершені, зокрема, обґрунтування зміни. [13]

Орган з сертифікації кібербезпеки повинен забезпечити, що:

а) внутрішні аудити проводяться персоналом, обізнаним щодо сертифікації продукції ІКТ, послуг ІКТ та процесів ІКТ, проведення аудитів та вимог стандарту ДСТУ EN ISO/IEC 17065;

б) аудитори не перевіряють свою власну роботу;

в) персонал, що відповідає за область, що піддається аудиту, поінформований щодо результатів аудиту;

г) будь-які дії за результатами внутрішніх аудитів вживаються своєчасно та належним чином;

д) визначаються будь-які можливості для поліпшування.

3.4.4 Процедура коригувальних та запобіжних дій органу з сертифікації кібербезпеки

Орган з сертифікації кібербезпеки повинен встановити процедури для ідентифікації та керування невідповідностями у своїй діяльності. [13]

Орган з сертифікації кібербезпеки повинен також, якщо необхідно, вжити заходів, щоб усунути причини невідповідностей для того для запобігання їх повторенню. [13]

Коригувальні дії повинні бути адекватними, щоб вплинути на виявлені проблеми.

Процедури для коригувальних дій повинні визначити вимоги до:

а) ідентифікації невідповідностей (наприклад, за результатами розгляду скарг і внутрішніх аудитів);

б) визначення причин невідповідності;

в) усунення невідповідностей;

г) оцінювання необхідності в діях для запобігання повторенню невідповідностей;

д) визначення і своєчасного впровадження необхідних дій;

е) реєстрування результатів виконаних дій;

ж) аналізування результативності коригувальних дій.

Орган з сертифікації кібербезпеки повинен встановити процедури для впровадження запобіжних дій, щоб усунути причини потенційних невідповідностей.

Вжиті запобіжні дії повинні бути адекватними можливим наслідкам потенційних проблем.

Процедури для запобіжних дій повинні визначити вимоги до:

а) ідентифікації потенційних невідповідностей та їх причин;

б) оцінювання потреби в діях, щоб запобігти виникненню невідповідностей;

в) визначення і впровадження необхідних дій;

г) реєстрування результатів виконаних дій;

д) аналізування результативності виконаних запобіжних дій. [13]

3.5 Висновки з розділу 3

В розділі визначено загальний порядок акредитації ООВ інформаційних та телекомунікаційних технологій в національній системі кібербезпеки України, які будуть відповідати вимогам Акту з кібербезпеки ЄС згідно Регламенту ЄС 2019/881, що почав діяти в Європейському Союзі з 2019 року.

В Україні такі ООВ повинні відповідати вимогам відповідного стандарту ДСТУ EN ISO/IEC 17065.

ООВ інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки є орган з сертифікації кібербезпеки продукції ІКТ, послуг ІКТ та

процесів ІКТ, який у відповідності до вимог стандарту ДСТУ EN ISO/IEC 17065 повинен бути юридичною особою або визначеною частиною юридичної особи і нести юридичну відповідальність за всю свою сертифікаційну діяльність.

Розглянуті в роботі вимоги до структури та ресурсів органу з сертифікації кібербезпеки, а також процедури сертифікації інформаційних та телекомунікаційних технологій на кібербезпеку, відповідають правовому полю системи технічного регулювання України та можуть бути застосовані для національної системи кібербезпеки України.

ВИСНОВКИ

У магістерській роботі наведено теоретичне узагальнення і нове вирішення наукового завдання, що полягає у вдосконаленні національної системи кібербезпеки України шляхом дослідження та розв‘язання проблем сертифікації інформаційних та телекомунікаційних технологій України щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

Метою роботи є вдосконалення національної системи кібербезпеки України в частині створення дієвої системи оцінки відповідності інформаційних та телекомунікаційних технологій в Україні щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС.

В роботі вирішені наступні задачі, які мають важливий практичний аспект:

а) досліджено шляхи забезпечення кібербезпеки та підвищення рівня довіри до цифрових технологій в ЄС шляхом оцінок відповідності;

б) досліджено роль Європейської системи сертифікації кібербезпеки у підвищенні довіри та безпеки до інформаційних та телекомунікаційних технологій у відповідності до Акту про кібербезпеку (Регламент ЄС 2019/881);

в) розроблені пропозиції з вдосконалення національної системи кібербезпеки України шляхом впровадження сертифікації інформаційних та телекомунікаційних технологій щодо кібербезпеки на відповідність вимогам Акту з кібербезпеки ЄС;

г) розроблені вимоги до структури та ресурсів органу з сертифікації кібербезпеки національної системи кібербезпеки України;

д) розроблені процедури сертифікації інформаційних та телекомунікаційних технологій в національній системі кібербезпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рекомендація Комісії від 6 травня 2003 року щодо визначення мікро-, малих та середніх підприємств (OB L 124, 20.5.2003, c. 36).

2. Регламент (ЄС) No 526/2013 Європейського Парламенту та Ради від 21 травня 2013 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про скасування Регламенту (ЄС) No 460/2004 (OB L 165 , 18.6.2013, c.41).

3. Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та про скасування Регламенту (ЄС) No 526/2013 (Закон про кібербезпеку).

4. Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи щодо високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (OB L 194, 19.7.2016, c. 1).

5. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних та про скасування Директиви 95 / 46 / ЄС (Загальний регламент про захист даних) (OB L 119, 4.5.2016, c. 1).

6. Рекомендація Комісії (ЄС) 2017/1584 від 13 вересня 2017 року щодо скоординованого реагування на масштабні інциденти та кризи в галузі кібербезпеки (OB L 239, 19.9.2017, c. 36).

7. Регламент (ЄС) No 765/2008 Європейського Парламенту та Ради від 9 липня 2008 року, що встановлює вимоги до акредитації та нагляду за ринком, що стосуються збуту продукції, та скасування Регламенту (ЄЕС) No 339/93 (OB L 218, 13.8.2008, c. 30).

8. Регламент (ЄС) No 1025/2012 Європейського Парламенту та Ради від 25 жовтня 2012 року про європейську стандартизацію, що вносить зміни до Директив Ради 89/686 / ЄЕС та 93/15 / ЄЕС та Директив 94/9 / ЄС, 94 / 25 / ЄС, 95/16 / ЄС, 97/23 / ЄС, 98/34 / ЄС, 2004/22 / ЄС, 2007/23 / ЄС, 2009/23 / ЄС та

2009/105 / ЄС Європейського Парламенту та Ради та скасування Рішення Ради 87/95 / ЄЕС та Рішення Європейського Парламенту та Ради No 1673/2006 / ЄС (OB L 316, 14.11.2012, c. 12).

9. ДСТУ EN ISO/IEC 17065:2014 Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг (EN ISO/IEC 17065:2012, IDT).

10. ISO/IEC 17000:2020 Conformity assessment - Vocabulary and general principles.

11. European Union Agency for Cybersecurity [Електронний ресурс]// – Режим доступу: https://www.enisa.europa.eu/topics/standards

12. International Organization for Standardization [Електронний ресурс]// – Режим доступу: http://www.iso.org/iso/home.html.

13. Національне агентство акредитації України [Електронний ресурс]// – Режим доступу: http://naau.org.ua/.